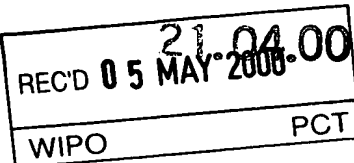


09/719 112

PCT/JP 00/02289

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 4月12日

出 願 番 号

Application Number:

平成11年特許願第103993号

出 願 人

Applicant (s):

ソニー株式会社

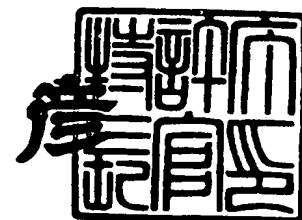
EKU

PRIORITY
DOCUMENTSUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 3月10日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3015810

【書類名】 特許願

【整理番号】 9900015709

【提出日】 平成11年 4月12日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 石橋 義人

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 大石 丈於

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 武藤 明宏

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

 【予納台帳番号】 032089

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに提供媒体

【特許請求の範囲】

【請求項 1】 暗号化されている第 1 の情報を保持する保持手段と、

前記第 1 の情報の利用条件と前記利用条件に対応する利用内容を含む第 2 の情報を、前記第 1 の情報に対応させて記憶する記憶手段と、

前記保持手段により保持されている暗号化されている前記第 1 の情報と、前記記憶手段により記憶されている前記第 2 の情報を所定のプロバイダに送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 暗号化されている第 1 の情報を保持する保持ステップと、

前記第 1 の情報の利用条件と前記利用条件に対応する利用内容を含む第 2 の情報を、前記第 1 の情報に対応させて記憶する記憶ステップと、

前記保持ステップで保持された暗号化されている前記第 1 の情報と、前記記憶ステップで記憶された前記第 2 の情報を所定のプロバイダに送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 3】 暗号化されている第 1 の情報を保持する保持ステップと、

前記第 1 の情報の利用条件と前記利用条件に対応する利用内容を含む第 2 の情報を、前記第 1 の情報に対応させて記憶する記憶ステップと、

前記保持ステップで保持された暗号化されている前記第 1 の情報と、前記記憶ステップで記憶された前記第 2 の情報を所定のプロバイダに送信する送信ステップと

を含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 4】 所定のプロバイダから送信されてくる、暗号化されている第 1 の情報、および前記第 1 の情報の利用条件と前記利用条件に対応する利用内容を含む第 2 の情報を受信する受信手段と、

前記受信手段により受信された前記第 2 の情報に対応して、前記第 1 の情報の

価格条件と前記価格条件に対応する価格内容を含む第3の情報を作成する作成手段と、

前記受信手段により受信された暗号化されている前記第1の情報および前記第2の情報、並びに前記作成手段により作成された前記第3の情報を、所定の機器に送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項5】 所定のプロバイダから送信されてくる、暗号化されている第1の情報、および前記第1の情報の利用条件と前記利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、

前記受信ステップで受信された前記第2の情報に対応して、前記第1の情報の価格条件と前記価格条件に対応する価格内容を含む第3の情報を作成する作成ステップと、

前記受信ステップで受信された暗号化されている前記第1の情報および前記第2の情報、並びに前記作成ステップで作成された前記第3の情報を、所定の機器に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項6】 所定のプロバイダから送信されてくる、暗号化されている第1の情報、および前記第1の情報の利用条件と前記利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、

前記受信ステップで受信された前記第2の情報に対応して、前記第1の情報の価格条件と前記価格条件に対応する価格内容を含む第3の情報を作成する作成ステップと、

前記受信ステップで受信された暗号化されている前記第1の情報および前記第2の情報、並びに前記作成ステップで作成された前記第3の情報を、所定の機器に送信する送信ステップと

を含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項7】 所定の基準情報を記憶する記憶手段と、

所定のプロバイダから送信されてくる、暗号化されている第1の情報、前記第

1 の情報の利用条件と前記利用条件に対応する利用内容を含む第 2 の情報、および前記第 1 の情報の価格条件と前記価格条件に対応する価格内容を含む第 3 の情報を受信する受信手段と、

前記記憶手段に記憶されている前記基準情報に対応する、前記受信手段により受信された前記第 2 の情報の前記利用条件を選択する利用条件選択手段と、

前記記憶手段に記憶されている前記基準情報に対応する、前記受信手段により受信された前記第 3 の情報の前記価格条件を選択する価格条件選択手段と、

前記利用条件選択手段により選択された前記利用条件に対応する前記利用内容に従って、暗号化されている前記第 1 の情報を復号して、利用する利用手段と、

前記価格条件選択手段により選択された前記価格条件に対応する前記価格内容に従って、前記利用手段による利用に対する課金処理を実行する実行手段とを備えることを特徴とする情報処理装置。

【請求項 8】 所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第 1 の情報、前記第 1 の情報の利用条件と前記利用条件に対応する利用内容を含む第 2 の情報、および前記第 1 の情報の価格条件と前記価格条件に対応する価格内容を含む第 3 の情報を受信する受信ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第 2 の情報の前記利用条件を選択する利用条件選択ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第 3 の情報の前記価格条件を選択する価格条件選択ステップと、

前記利用条件選択ステップで選択された前記利用条件に対応する前記利用内容に従って、暗号化されている前記第 1 の情報を復号して、利用する利用ステップと、

前記価格条件選択ステップで選択された前記価格条件に対応する前記価格内容に従って、前記利用ステップでの利用に対する課金処理を実行する実行ステップと

を含むことを特徴とする情報処理方法。

【請求項 9】 所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第1の情報、前記第1の情報の利用条件と前記利用条件に対応する利用内容を含む第2の情報、および前記第1の情報の価格条件と前記価格条件に対応する価格内容を含む第3の情報を受信する受信ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第2の情報の前記利用条件を選択する利用条件選択ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第3の情報の前記価格条件を選択する価格条件選択ステップと、

前記利用条件選択ステップで選択された前記利用条件に対応する前記利用内容に従って、暗号化されている前記第1の情報を復号して、利用する利用ステップと、

前記価格条件選択ステップで選択された前記価格条件に対応する前記価格内容に従って、前記利用ステップでの利用に対する課金処理を実行する実行ステップと

を含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

【0002】

【従来技術】

音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、その情報処理装置でコンテンツを復号して、利用するシステムがある。

【0003】

【発明が解決しようとする課題】

しかしながら、従来のシステムにおいては、ユーザの性別や年齢などの個人情報

報、コンテンツの利用実績、またはユーザの所有する情報処理装置の種類に応じて、コンテンツの利用を提供するなど、変化に富んだサービスを提供することができない課題があった。

【0004】

本発明はこのような状況に鑑みてなされたものであり、変化に富んだサービスを提供することができるようにするものである。

【0005】

【課題を解決するための手段】

請求項1に記載の情報処理装置は、暗号化されている第1の情報を保持する保持手段と、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を、第1の情報に対応させて記憶する記憶手段と、保持手段により保持されている暗号化されている第1の情報と、記憶手段により記憶されている第2の情報を所定のプロバイダに送信する送信手段とを備えることを特徴とする。

【0006】

請求項2に記載の情報処理方法は 暗号化されている第1の情報を保持する保持ステップと、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を、第1の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第1の情報と、記憶ステップで記憶された第2の情報を所定のプロバイダに送信する送信ステップとを含むことを特徴とする。

【0007】

請求項3に記載の提供媒体は、暗号化されている第1の情報を保持する保持ステップと、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を、第1の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第1の情報と、記憶ステップで記憶された第2の情報を所定のプロバイダに送信する送信ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0008】

請求項1に記載の情報処理装置、請求項2に記載の情報処理方法、および請求項3に記載の提供媒体においては、暗号化されている第1の情報が保持され、第

1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報が、第1の情報に対応されて記憶され、保持された暗号化されている第1の情報と、記憶された第2の情報が所定のプロバイダに送信される。

【0009】

請求項4に記載の情報処理装置は、所定のプロバイダから送信されてくる、暗号化されている第1の情報、および第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を受信する受信手段と、受信手段により受信された第2の情報に対応して、第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を作成する作成手段と、受信手段により受信された暗号化されている第1の情報および第2の情報、並びに作成手段により作成された第3の情報を、所定の機器に送信する送信手段とを備えることを特徴とする。

【0010】

請求項5に記載の情報処理方法は、所定のプロバイダから送信されてくる、暗号化されている第1の情報、および第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、受信ステップで受信された第2の情報に対応して、第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を作成する作成ステップと、受信ステップで受信された暗号化されている第1の情報および第2の情報、並びに作成ステップで作成された第3の情報を、所定の機器に送信する送信ステップとを含むことを特徴とする。

【0011】

請求項6に記載の提供媒体は、所定のプロバイダから送信されてくる、暗号化されている第1の情報、および第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、受信ステップで受信された第2の情報に対応して、第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を作成する作成ステップと、受信ステップで受信された暗号化されている第1の情報および第2の情報、並びに作成ステップで作成された第3の情報を、所定の機器に送信する送信ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0012】

請求項 4 に記載の情報処理装置、請求項 5 に記載の情報処理方法、および請求項 6 に記載の提供媒体においては、所定のプロバイダから送信されてくる、暗号化されている第 1 の情報、および第 1 の情報の利用条件と利用条件に対応する利用内容を含む第 2 の情報が受信され、受信された第 2 の情報に対応して、第 1 の情報の価格条件と価格条件に対応する価格内容を含む第 3 の情報が作成され、受信された暗号化されている第 1 の情報および第 2 の情報、並びに作成された第 3 の情報が、所定の機器に送信される。

【0013】

請求項 7 に記載の情報処理装置は、所定の基準情報を記憶する記憶手段と、所定のプロバイダから送信されてくる、暗号化されている第 1 の情報、第 1 の情報の利用条件と利用条件に対応する利用内容を含む第 2 の情報、および第 1 の情報の価格条件と価格条件に対応する価格内容を含む第 3 の情報を受信する受信手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第 2 の情報の利用条件を選択する利用条件選択手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第 3 の情報の価格条件を選択する価格条件選択手段と、利用条件選択手段により選択された利用条件に対応する利用内容に従って、暗号化されている第 1 の情報を復号して、利用する利用手段と、価格条件選択手段により選択された価格条件に対応する価格内容に従って、利用手段による利用に対する課金処理を実行する実行手段とを備えることを特徴とする。

【0014】

請求項 8 に記載の情報処理方法は、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第 1 の情報、第 1 の情報の利用条件と利用条件に対応する利用内容を含む第 2 の情報、および第 1 の情報の価格条件と価格条件に対応する価格内容を含む第 3 の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第 2 の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第 3 の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された

利用条件に対応する利用内容に従って、暗号化されている第1の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップとを含むことを特徴とする。

【0015】

請求項9に記載の提供媒体は、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第1の情報、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報、および第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第2の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第3の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された利用条件に対応する利用内容に従って、暗号化されている第1の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0016】

請求項7に記載の情報処理装置、請求項8に記載の情報処理方法、および請求項9に記載の提供媒体においては、所定の基準情報が記憶され、所定のプロバイダから送信されてくる、暗号化されている第1の情報、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報、および第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報が受信され、記憶されている基準情報に対応する、受信された第2の情報の利用条件が選択され、記憶されている基準情報に対応する、受信された第3の情報の価格条件が選択され、選択された利用条件に対応する利用内容に従って、暗号化されている第1の情報が復号され、利用され、選択された価格条件に対応する価格内容に従って、利用に対する課金処理が実行される。

【0017】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0018】

図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ1、コンテンツを提供するコンテンツプロバイダ2、コンテンツに対応する所定のサービスを提供するサービスプロバイダ3、およびコンテンツが利用される機器（この例の場合、レシーバ51およびレシーバ201）からなるユーザホームネットワーク5から構成されている。

【0019】

EMDシステムに登録された機器（例えば、レシーバ51またはレシーバ201）に配信（提供）されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。ユーザは、コンテンツを購入し（実際は、コンテンツを利用する権利を購入し）、提供されるコンテンツを再生したり、複製して利用する。

【0020】

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5、および複数のコンテンツプロバイダ2（この例の場合、2式のコンテンツプロバイダ2-1, 2-2（以下、コンテンツプロバイダ2-1, 2-2を個々に区別する必要がある場合、単に、コンテンツプロバイダ2と記述する。他の装置についても同様である））に、コンテンツを利用するために必要な配送用鍵Kdを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算したり、コンテンツプロバイダ2からはUCPを、そしてサービスプロバイダ3か

らPTを受信する。

【0021】

コンテンツプロバイダ2-1, 2-2は、提供するコンテンツ（コンテンツ鍵Kc oで暗号化されている）、そのコンテンツを復号するために必要なコンテンツ鍵Kc o（配送用鍵Kdで暗号化されている）、およびコンテンツの利用内容などを示す取扱方針（以下、UCP(Usage Control Policy)と記述する）を保持し、それらを、コンテンツプロバイダセキュアコンテナ（後述）と称する形態で、サービスプロバイダ3に供給する。なお、この例の場合、2式のサービスプロバイダ3-1, 3-2が存在するものとする。

【0022】

サービスプロバイダ3-1, 3-2は、コンテンツプロバイダ2から供給されるUCPに対応して、1つまたは複数の価格情報（以下、PT(Price Tag)と記述する）を作成し、それを保持する。サービスプロバイダ3は、作成したPTを、コンテンツプロバイダ2から供給されたコンテンツ（コンテンツ鍵Kc oで暗号化されている）、コンテンツ鍵Kc o（配送用鍵Kdで暗号化されている）、およびUCPとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、ユーザホームネットワーク5に送信する。

【0023】

ユーザホームネットワーク5は、供給されたUCPおよびPTに基づいて、使用許諾条件情報（以下、UCS(Usage Control Status)と称する）を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク5はまた、UCSを作成するタイミングで課金情報を作成し、例えば、配送用鍵Kdの供給を受けるタイミングで、対応するUCPおよびPTなどとともにEMDサービスセンタ1に送信する。なお、ユーザホームネットワーク5は、UCPおよびPTをEMDサービスセンタ1に送信しないようにすることもできる。

【0024】

この例の場合、ユーザホームネットワーク5は、図1に示すように、HDD52に接続され、SAM62を有するレシーバ51、およびHDD202に接続され、SAM

212を有するレシーバ201から構成されている。なお、レシーバ51およびレシーバ201についての詳細は後述する。

【0025】

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信したり、利益分配の情報を供給する。

【0026】

著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)に送信する。

【0027】

鍵サーバ14は、配送用鍵Kdを記憶しており、それを、コンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給したり、ユーザ管理部18等を介してユーザホームネットワーク5に供給する。

【0028】

ユーザホームネットワーク5の、EMDシステムに正式登録された機器およびコンテンツプロバイダ2に供給される、EMDサービスセンタ1からの配送用鍵Kdについて、図4乃至図7を参照して説明する。

【0029】

図4は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成する、例えば、レシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵Kd、コンテンツプロバイダ2が有する配送用鍵Kd、およびレシーバ51が有する配送用鍵Kdを示す図である。

【0030】

図4の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可

能であり、たとえば、所定のビット数の乱数である” a a a a a a a a ” の値を有するバージョン1である配送用鍵K d は、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵K c o は、バージョン1である配送用鍵K d で暗号化されている）であり、所定のビット数の乱数である” b b b b b b b b ” の値を有するバージョン2である配送用鍵K d は、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵K c o は、バージョン2である配送用鍵K d で暗号化されている）である。同様に、バージョン3である配送用鍵K d は、1998年3月中に使用可能であり、バージョン4である配送用鍵K d は、1998年4月中に使用可能であり、バージョン5である配送用鍵K d は、1998年5月中に使用可能であり、バージョン6である配送用鍵K d は、1998年6月中に使用可能である。

【0031】

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵K d を送信し、コンテンツプロバイダ2は、6つの配送用鍵K d を受信し、記憶する。6月分の配送用鍵K d を記憶するのは、コンテンツプロバイダ2が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【0032】

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵K d を送信し、レシーバ51は、3つの配送用鍵K d を受信し、記憶する。3月分の配送用鍵K d を記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブル

ルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

【0033】

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0034】

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

【0035】

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0036】

1998年3月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月

まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdおよびバージョン2である配送用鍵Kdをそのまま記憶する。

【0037】

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0038】

1998年4月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図7で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kd、バージョン2である配送用鍵Kd、およびバージョン3である配送用鍵Kdをそのまま記憶する。

【0039】

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホ

ームネットワーク 5 を構成するレシーバ 51 で利用される。

【0040】

このように、あらかじめ先の月の配送用鍵 K d を配布しておくことで、仮にユーザが 1, 2 ヶ月まったく EMD サービスセンタ 1 にアクセスしなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMD サービスセンタ 1 にアクセスして鍵を受信することができる。

【0041】

また、ユーザホームネットワーク 5 の、EMD システムに正式登録された機器、およびコンテンツプロバイダ 2 には、以上のように、3 ヶ月分の配送用鍵 K d が配布されるが、EMD システムに正式登録されておらず、仮登録（詳細は後述する）されている状態の、ユーザホームネットワーク 5 の機器には、3 ヶ月分の配送用鍵 K d に代わり、図 8 に示すような、1 ヶ月分の配送用鍵 K d が配布される。この例においては、ユーザホームネットワーク 5 の機器を EMD システムに正式登録するために、与信処理など、約 1 月程度の時間を有する登録手続が必要となる。そこで、登録申請から正式登録されるまでの間（約 1 ヶ月間）においても、コンテンツの利用が可能となるように、正式登録されていない機器（仮登録されている機器）には、1 ヶ月間において利用可能な配送用鍵 K d が配布される。

【0042】

図 3 に戻り、経歴データ管理部 15 は、ユーザ管理部 18 から出力される、課金情報、そのコンテンツに対応する PT、およびそのコンテンツに対応する UCP などを記憶する。

【0043】

利益分配部 16 は、経歴データ管理部 15 から供給された各種情報に基づき、EMD サービスセンタ 1、コンテンツプロバイダ 2-1, 2-2、およびサービスプロバイダ 3-1, 3-2 の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部 11、コンテンツプロバイダ管理部 12、出納部 20、および著作権管理部 13 に出力する。利益配分部 16 はまた、算出した利益に応じてコンテンツプロバイダ 2-1, 2-2 およびサービスプロバイダ 3-1, 3-2 のそれぞれに対する利用ポイント（利益が大きければ大きいほど、すなわち、ユーザが利

用すればするほど、大きい値となるポイント)を算出し、ユーザ管理部18に出力する。なお、以下において、コンテンツプロバイダ2における利用ポイントをコンテンツ利用ポイントと称し、サービスプロバイダ3における利用ポイントをサービス利用ポイントと称する。

【0044】

相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の機器と相互認証を実行する。

【0045】

ユーザ管理部18は、EMDシステムに登録可能な、ユーザホームネットワーク5の機器に関する情報(以下、システム登録情報と称する)を管理する。システム登録情報には、図9に示すように、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に設定される情報が含まれる。

【0046】

「SAMのID」には、製造された、ユーザホームネットワーク5の機器のSAMのIDが記憶される。図9のシステム登録情報の「SAMのID」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDが設定されている。

【0047】

「機器番号」には、SAMを有するユーザホームネットワーク5の機器に、予め設定された機器番号が設定される。ユーザホームネットワーク5の機器が、ネットワーク4を介してサービスプロバイダ3と、およびEMDサービスセンタ1と直接通信することができる機能を有し(通信部を有し)、かつ、例えば、UCPやPTの内容をユーザに出力(提示)したり、ユーザがUCPの利用内容を選択することができる機能を有している(表示部および操作部を有している)場合、その機器(以下、このような機能を有する機器を主機器と称する)には、100番以上の機器番号が与えられる。機器が、そのような機能を有しない場合、その機器(以下、このような機器を従機器と称する)には、99番以下の機器番号が与えられる。この例の場合、レシーバ51およびレシーバ201の両者は、上述した機能を有しているので、それぞれには、100番以上の機器番号(100番)が与

えられてる。そこで、図9のシステム登録情報の「機器番号」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDに対応する「機器番号」のそれぞれには、機器番号100番が設定されている。

【0048】

「決済ID」には、EMDシステムに正式登録されたとき割り当てられる所定のIDが記憶される。この例の場合、レシーバ51は、ユーザFが決済ユーザ（後述）として、そしてレシーバ201は、ユーザAを決済ユーザとして、それぞれ正式登録され、決済IDが与えられているので、図9のシステム登録情報の、SAM62のIDおよびSAM212のIDに対応する「決済ID」には、与えられた決済IDが設定されている。

【0049】

「決済ユーザ情報」には、計上される課金を決済するユーザ（以下、このようなユーザを決済ユーザと称する）の、氏名、住所、電話番号、決済機関情報（例えば、クレジットカード番号等）、生年月日、年齢、性別、ID、パスワードなどが設定される。

【0050】

「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、および性別（以下、「決済ユーザ情報」に設定されるこれらの情報を、個々に区別する必要がない場合、まとめて、ユーザー一般情報と称する）は、登録が申請される際にユーザから提供され、設定されるが、この例の場合、そのうちの、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対してユーザー一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、IDおよびパスワードは、EMDシステムに仮登録されるときに割り当てられ、設定される。

【0051】

この例の場合、レシーバ51は、ユーザFが決済ユーザとして登録されている

ので、図9のシステム登録情報の、SAM62のIDに対応する「決済ユーザ情報」には、ユーザFから提供されたユーザ一般情報、ユーザFのID、およびユーザFのパスワードが設定されている。レシーバ201は、ユーザAが決済ユーザとして登録されているので、SAM212のIDに対応する「決済ユーザ情報」には、ユーザAから提供されたユーザ一般情報、ユーザAのID、およびユーザAのパスワードが設定されている。なお、この例の場合、ユーザFは、男性で、ユーザAは、女性とする。

【0052】

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ID、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情報のうち、決済機関の情報以外の情報が設定される。従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、IDおよびパスワードは、仮登録または正式登録されるときに割り当てられ、設定される。

【0053】

この例の場合、レシーバ51およびレシーバ201の両者には、従属ユーザが登録されていないので、図9のシステム登録情報のSAM62のIDに対応する「従属ユーザ情報」、およびSAM212のIDに対応する「従属ユーザ情報」には、何の情報も設定されていない。

【0054】

「利用ポイント情報」には、利益分配部16から出力された利用ポイントが設定される。図10(A)は、SAM62に対応する「利用ポイント情報」に記憶されているレシーバ51の利用ポイント情報を示している。これによれば、レシーバ51のユーザF（決済ユーザ）には、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイント、コンテンツプロバイダ2-2のコンテンツ利

用ポイントが123ポイント、サービスプロバイダ3-1のサービス利用ポイントが345ポイント、そしてサービスプロバイダ3-2のサービス利用ポイントが0ポイントだけ与えられている。

【0055】

図10(B)は、SAM212に対応する「利用ポイント情報」に記憶されているレシーバ201の利用ポイント情報を示している。これによれば、レシーバ201のユーザA(決済ユーザ)には、コンテンツプロバイダ2-1のコンテンツ利用ポイントが23ポイント、コンテンツプロバイダ2-2のコンテンツ利用ポイントが22ポイント、サービスプロバイダ3-1のサービス利用ポイントが40ポイント、そしてサービスプロバイダ3-2のサービス利用ポイントが5ポイントだけ与えられている。

【0056】

なお、この例において、コンテンツプロバイダ2-1およびコンテンツプロバイダ2-2のそれぞれのコンテンツ利用ポイントの合計ポイント(ユーザFの場合は345($=123+222$)、ユーザAの場合は45ポイント($=23+22$))と、サービスプロバイダ3-1およびサービスプロバイダ3-2のそれぞれのサービス利用ポイントの合計ポイント(ユーザFの場合は345($=345+0$)、ユーザAの場合は45ポイント($=5+40$))が等しくなるようになされている。

【0057】

ユーザ管理部18は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト(後述)を作成し、配送用鍵Kdとともにユーザホームネットワーク5に送信する。

【0058】

図3に、再度戻り、課金請求部19は、経歴データ管理部15から供給された、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部20はまた、決算処理の結

果をユーザ管理部 18 に通知する。

【0059】

監査部 21 は、ユーザホームネットワーク 5 の機器から供給された課金情報、PT、および UCP の正当性（すなわち、不正をしていないか）を監査する。なお、この場合、EMD サービスセンタ 1 は、コンテンツプロバイダ 2 からの UCP を、サービスプロバイダ 3 からの PT を、そしてユーザホームネットワーク 5 からの UCP と PT を、それぞれ受け取る。

【0060】

図 11 は、コンテンツプロバイダ 2-1 の機能的構成を示すブロック図である。コンテンツサーバ 31 は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部 32 に供給する。ウォーターマーク付加部 32 は、コンテンツサーバ 31 から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部 33 に供給する。

【0061】

圧縮部 33 は、ウォーターマーク付加部 32 から供給されたコンテンツを、ATRA C2 (Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵（以下、この乱数をコンテンツ鍵 K_c と称する）として、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0062】

乱数発生部 35 は、コンテンツ鍵 K_c となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵 K_c を EMD サービスセンタ 1 から供給された配送用鍵 K_d を使用して、DES などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0063】

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する

部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【 0 0 6 4 】

まず、平文の64ビットは、上位32ビットの H_0 、および下位32ビットの L_0 に分割される。鍵処理部から供給された48ビットの拡大鍵 K_1 、および下位32ビットの L_0 を入力とし、下位32ビットの L_0 を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットの H_0 と、F関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

【 0 0 6 5 】

上位32ビットの H_0 および下位32ビットの L_0 を基に、以上の処理を16回繰り返し、得られた上位32ビットの H_{16} および下位32ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【 0 0 6 6 】

ポリシー記憶部37は、コンテンツに対応して設定されるUCPを記憶し、セキュアコンテナ作成部38に出力する。図12は、コンテンツサーバ31に保持されているコンテンツAに対応して設定され、ポリシー記憶部37に記憶されているUCPA、Bを表している。UCPには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「利用条件」、「利用内容」の各項目に設定される情報が含まれる。「コンテンツのID」には、UCPが対応するコンテンツのIDが設定される。UCPA（図12（A））およびUCPB（図12（B））のそれぞれの「コンテンツのID」には、コンテンツAのIDが設定されている。

【 0 0 6 7 】

「コンテンツプロバイダのID」には、コンテンツの提供元のコンテンツプロバイダのIDが設定される。UCPAおよびUCPBのそれぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが設定されている。「UCPのID」

には、各UCPに割り当てられた所定のIDが設定され、UCPAの「UCPのID」には、UCPAのIDが、UCPBの「UCPのID」には、UCPBのIDが、それぞれ設定されている。「UCPの有効期限」には、UCPの有効期限を示す情報が設定され、UCPAの「UCPの有効期限」には、UCPAの有効期限が、UCPBの「UCPの有効期限」には、UCPBの有効期限が、それぞれ設定されている。

【0068】

「利用条件」は、「ユーザ条件」および「機器条件」の項目からなり、「ユーザ条件」には、このUCPを選択することができるユーザの条件が設定され、「機器条件」には、このUCPを選択することができる機器の条件が設定される。

【0069】

UCPAの場合、「利用条件10」が設定され、「利用条件10」の「ユーザ条件10」には、利用ポイントが200ポイント以上であることが条件であることを示す情報（“200ポイント以上”）が設定されている。また「利用条件10」の「機器条件10」には、条件がないことを示す情報（“条件なし”）が設定されている。すなわち、UCPAは、200ポイント以上のコンテンツプロバイダ2-1のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

【0070】

UCPBの場合、「利用条件20」が設定され、「利用条件20」の「ユーザ条件20」には、利用ポイントが200ポイントより少ないことが条件であることを示す情報（“200ポイントより少ない”）が設定されている。また「利用条件20」の「機器条件20」には、“条件なし”が設定されている。すなわち、UCPBは、200ポイントより少ないコンテンツプロバイダ2-1のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

【0071】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」などの項目からなり、その「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

【0072】

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報（”可”または”不可”）が設定されている。コンテンツの管理移動が行われると、図13（A）に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図13（B）に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

【0073】

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図13（A）に示すように、他の機器にコンテンツを管理移動することができない（許可されない）。すなわち、管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。この点で、図14（A）に示すように、オリジナルのコンテンツから、複数の複製（第1世代）を作成することができる、第1世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図14（B）に示すように、1回だけの複製とも異なる。

【0074】

図12（A）に戻り、UCPAには、4つの「利用内容11」乃至「利用内容14」が設けられており、「利用内容11」において、その「ID11」には、「利用内容11」に割り当てられた所定のIDが設定されている。「形式11」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ11」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報11」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

【0075】

「利用内容12」において、その「ID12」には、「利用内容12」に割り当てられた所定のIDが設定されている。「形式12」には、第1世代の複製を行う

利用形式を示す情報（”第1世代複製”）が設定されている。第1世代複製は、図14（A）に示したように、オリジナルのコンテンツから、複数の第1世代の複製を作成することができる。ただし、第1世代の複製から第2世代の複製を作成することはできない（許可されない）。「パラメータ12」には、”第1世代複製”に対応する所定の情報が設定されている。「管理移動許可情報12」には、コンテンツの管理移動が許可されていないことを示す”不可”が設定されている。

【0076】

「利用内容13」において、その「ID13」には、「利用内容13」に割り当てられた所定のIDが設定されている。「形式13」には、所定の期間（時間）に限って再生する利用形式を示す情報（”期間制限再生”）が設定され、「パラメータ13」には、”期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報13」には、”不可”が設定されている。

【0077】

「利用内容14」において、その「ID14」には、「利用内容14」に割り当てられた所定のIDが設定されている。「形式14」には、5回の複製を行う利用形式（いわゆる、5回複製することができる回数券）を示す情報（”Pay Per Copy5”）が設定されている。なお、この場合も、図14の（B）に示すように、複製からの複製を作成することはできない（許可されない）。「パラメータ14」には、”Pay Per Copy5”に対応して、複製が5回可能であることを示す情報”複製5回”が設定されている。「管理移動許可情報14」には、”不可”が設定されている。

【0078】

図12（B）のUCPBには、2つの「利用内容21」および「利用内容22」が設けられている。「利用内容21」において、その「ID21」には、「利用内容21」に割り当てられた所定のIDが設定されている。「形式21」には、4回の再生を行う利用形式を示す情報（”Pay Per Play4”）が設定され、「パラメータ21」には、再生が4回可能であることを示す情報（”再生4回”）が設定

されている。「管理移動許可情報 2 1」には、「不可」が設定されている。

【0 0 7 9】

「利用内容 2 2」において、その「ID 2 2」には、「利用内容 2 2」に割り当てられた所定のIDが設定されている。「形式 2 2」には、「Pay Per Copy 2」が設定され、「パラメータ 2 2」には、「複製 2 回」が設定されている。「管理移動許可情報 2 2」には、「不可」が設定されている。

【0 0 8 0】

ここで、UCPAおよびUCPBの内容を比較すると、200ポイント以上の利用ポイントを有するユーザは、4通りの利用内容 1 1乃至利用内容 1 4から利用内容を選択することができるのに対して、200ポイントより少ない利用ポイントを有するユーザは、2通りの利用内容 2 1, 2 2からしか利用内容を選択することができないものとされている。

【0 0 8 1】

ところで、図 1 2 は、UCPAおよびUCPBを模擬的に表しているが、例えば、UCPAの「利用条件 1 0」およびUCPBの「利用条件 2 0」は、図 1 5 (A) に示すサービスコード、および図 1 5 (B) に示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードにより、実際は構成されている。

【0 0 8 2】

図 1 6 (A) は、UCPA (図 1 2 (A)) の「利用条件 1 0」の「ユーザ条件 1 0」および「機器条件 1 0」として設定されている各コードのコード値を表している。UCPAの「利用条件 1 0」の「ユーザ条件 1 0」は、「200ポイント以上」とされているので、「利用ポイントに関し条件有り」を意味する 8 0 x x h のサービスコード (図 1 5 (A)) が、このとき数値 2 0 0 を示す 0 0 0 0 C 8 h のバリューコードが、そして「>= (以上)」を意味する 0 6 h のコンディションコード (図 1 5 (B)) が、ユーザ条件として設定されている。

【0 0 8 3】

UCPAの「機器条件 1 0」は、「条件なし」とされているので、「条件なし」を意味する 0 0 0 0 h のサービスコードが、このとき何ら意味を持たない F F F

FFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが、機器条件として設定されている。

【0084】

図16(B)は、UCPBの「利用条件20」の「ユーザ条件20」および「機器条件20」として設定されている各コードのコード値を表している。「ユーザ条件20」は、”200ポイントより少ない”とされているので、”利用ポイントに関し条件有り”を意味する80xxhのサービスコードが、数値200を示す0000C8hのバリューコードが、そして”<(より小さい)”を意味する03hのコンディションコードが、ユーザ条件として設定されている。

【0085】

UCPBの「機器条件20」は、UCPAの「機器条件10」と同様に、”条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

【0086】

図11に戻り、セキュアコンテナ作成部38は、例えば、図17に示すような、コンテンツA(コンテンツ鍵Kc o Aで暗号化されている)、コンテンツ鍵Kc o A(配送用鍵Kdで暗号化されている)、UCPA、B、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ(この場合、コンテンツA(コンテンツ鍵Kc o Aで暗号化されている)、コンテンツ鍵Kc o A(配送用鍵Kdで暗号化されている)、およびUCPA、Bの全体)にハッシュ関数を適用して得られたハッシュ値が、公開鍵暗号の秘密鍵(この場合、コンテンツプロバイダ2-1の秘密鍵Ksc p)で暗号化されたものである。

【0087】

セキュアコンテナ作成部38はまた、コンテンツプロバイダセキュアコンテナに、図18に示すコンテンツプロバイダ2-1の証明書を付してサービスプロバイダ3に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2-1に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ2-1の名前、コンテンツプロバイダ2-1の公開鍵Kpc p、並びに

その署名（認証局の秘密鍵 K_{sca} で暗号化されている）から構成されている。

【0088】

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0089】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0090】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4、MD5、SHA-1などが用いられる。

【0091】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0092】

公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積で

ある n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3 以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1 のみである）。

【0093】

次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed=1 \bmod L$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p, q , および d が、秘密鍵とされる。

【0094】

暗号文 C は、平文 M から、式 (1) の処理で算出される。

【0095】

$$C = M^e \bmod n \quad (1)$$

暗号文 C は、式 (2) の処理で平文 M に、復号される。

【0096】

$$M = C^d \bmod n \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式 (3) が成立するからである。

【0097】

$$M = C^d = (M^e)^d = M^{ed} = M \bmod n \quad (3)$$

秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0098】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2 = x^3 + ax + b$ 上の、ある点を B とする。楕円曲線上の点の加算を定義し、 nB は、 B を n 回加算した結果を表す。同様に、減算も定義する。 B と nB から n を算出することは、困難であることが証明されている。 B と nB を公開鍵とし、 n を秘密鍵とする。乱数 r を用いて、暗号文 $C1$ および $C2$ は、平文 M から、公開鍵で式 (4)

および式(5)の処理で算出される。

【0099】

$$C1 = M + rnB \quad (4)$$

$$C2 = rB \quad (5)$$

暗号文C1およびC2は、式(6)の処理で平文Mに、復号される。

【0100】

$$M = C1 - nC2 \quad (6)$$

復号できるのは、秘密鍵 n を有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0101】

図11に、再び戻り、コンテンツプロバイダ2-1の相互認証部39は、EMDサービスセンタ1から配送用鍵 K_d の供給を受けるのに先立ち、EMDサービスセンタ1と相互認証し、また、相互認証部39は、サービスプロバイダ3へのコンテンツセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密にしなければならない情報が含まれていないので、この相互認証は、必ずしも必要とされない。

【0102】

コンテンツプロバイダ2-2は、コンテンツプロバイダ2-1と基本的の同様の構成を有しているので、その図示および説明は省略する。

【0103】

次に、図19のブロック図を参照して、サービスプロバイダ3-1の機能的構成を説明する。コンテンツサーバ41は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ(コンテンツ鍵 K_{co} で暗号化されている)、コンテンツ鍵 K_{co} (配送用鍵 K_d で暗号化されている)、UCP、およびコンテンツプロバイダ2の署名を記憶し、セキュアコンテナ作成部44に供給する。

【0104】

値付け部42は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ2の証明書が検証され、正当であるとき、コンテンツプロバイダ2の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

【0105】

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部42は、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部44に供給する。図20は、図12(A)のUCP Aに対応して作成された、2つのPTA-1(図20(A))およびPTA-2(図20(B))を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に設定される情報が含まれる。

【0106】

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのID」には、UCPに対応する各項目の情報が、それぞれ設定される。すなわち、PTA-1およびPTA-2のそれぞれの「コンテンツのID」には、コンテンツAのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが、そしてそれぞれの「UCPのID」には、UCPAのIDが設定されている。

【0107】

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ3のIDが設定される。PTA-1およびPTA-2の「サービスプロバイダのID」には、サービスプロバイダ3-1のIDが設定されている。「PTのID」には、各PTに割り当てられた所定のIDが設定される。PTA-1の「PTのID」には、PTA-1のIDが、PTA-2の「PTのID」には、PTA-2のIDがそれぞれ設定されている。「PTの有効期限」には、PTの有効期限を示す情報が設定される。PTA-1の「PTの有効期限」には、PTA-1の有効期限が、PTA-2の「PTの有効期限」には、PTA-2の

有効期限が設定されている。

【0108】

「価格条件」は、UCPの「利用条件」と同様に、「ユーザ条件」および「機器条件」の項目からなり、その「ユーザ条件」には、このPTを選択することができるユーザの条件が設定され、その「機器条件」には、このPTを選択することができる機器の条件が設定される。

【0109】

PTA-1の場合、「価格条件10」が設定され、「価格条件10」の「ユーザ条件10」には、ユーザが男性であることを示す情報（”男性”）が設定され、その「機器条件10」には、”条件なし”が設定されている。すなわち、PTA-1は、男性のユーザのみが選択可能となる。

【0110】

PTA-1の「価格条件10」の「ユーザ条件10」および「機器条件10」も、実際は、図21（A）に示すように、各種コードのコード値が設定されている。「価格条件10」の「ユーザ条件10」には、”性別条件有り”を意味する01xxhのサービスコード（図15（A））が、このとき男性を意味する000000hのバリューコードが、そして”=”を意味する01hのコンディションコード（図15（B））が設定されている。「機器条件10」には、”条件なし”を意味する0000hのサービスコードが、この場合何ら意味を持たないFFFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが設定されている。

【0111】

PTA-2の場合、「価格条件20」が設定され、「価格条件20」の「ユーザ条件20」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件20」には、”条件なし”が設定されている。すなわち、PTA-2は、女性のユーザのみが選択可能となる。

【0112】

PTA-2の「価格条件20」の「ユーザ条件20」および「機器条件20」も、実際は、図21（B）に示すように、各コードのコード値が設定されている。

「価格条件 20」の「ユーザ条件 20」には、“性別条件有り”を意味する 01 x x h のサービスコード（図 15（A））が、この場合女性を示す 000001 h のバリューコードが、そして“=”を意味する 01 h のコンディションコード（図 15（B））が設定されている。その「機器条件 20」には、“条件なし”を意味する 0000 h のサービスコードが、この場合何ら意味を持たない F F F F F F h のバリューコードが、そして“無条件”を意味する 00 h のコンディションコードが設定されている。

【0113】

図 20 に戻り、PT の「価格内容」には、コンテンツが、対応する UCP の「利用内容」の「形式」に設定された利用形式で利用される場合の利用料金が示されている。すなわち、PTA-1 の「価格内容 11」に設定された“2000 円”および PTA-2 の「価格内容 21」に設定された“1000 円”は、UCPA（図 12（A））の「利用内容 11」の「形式 11」が“買い取り再生”とされているので、コンテンツ A の買い取り価格（料金）を示している。

【0114】

PTA-1 の「価格内容 12」の“600 円”および PTA-2 の「価格内容 22」の“300 円”は、UCPA の「利用内容 12」の「形式 12」より、第 1 世代複製の利用形式でコンテンツ A を利用する場合の料金を示している。PTA-1 の「価格内容 13」の“100 円”および PTA-2 の「価格内容 23」の“50 円”は、UCPA の「利用内容 13」の「形式 13」より、期間制限再生の利用形式でコンテンツ A を利用する場合の料金を示している。PTA-1 の「価格内容 14」の“300 円”および PTA-2 の「価格内容 24」の“150 円”は、UCPA の「利用内容 14」の「形式 14」より、5 回の複製を行う利用形式でコンテンツ A を利用する場合の料金を示している。

【0115】

なお、この例の場合、PTA-1（男性ユーザに適用される）の価格内容と、PTA-2（女性ユーザに適用される）の価格内容を比較すると、PTA-1 の価格内容に示される価格が、PTA-2 の価格内容に示される価格の 2 倍に設定されている。例えば、UCPA の「利用内容 11」に対応する PTA-1 の「価格内容 11」

が”2000円”とされているのに対し、同様にUCPAの「利用内容11」に対応するPTA-2の「価格内容21」は”1000円”とされている。同様、PTA-1の「価格内容12」乃至「価格内容14」に設定されている価格は、PTA-2の「価格内容22」乃至「価格内容24」に設定されている価格のそれぞれの2倍とされている。すなわち、女性ユーザは、男性ユーザに比べ、コンテンツAを、半額の料金で利用することができる。

【0116】

図22は、図12(B)のUCPBに対応して作成された、2つのPTB-1およびPTB-2を表している。図22(A)のPTB-1には、コンテンツAのID、コンテンツプロバイダ2-1のID、UCPBのID、UCPBの有効期限、サービスプロバイダ3-1のID、PTB-1のID、PTB-1の有効期限、価格条件30、2通りの価格内容31、32などが含まれている。

【0117】

PTB-1の「価格条件30」の「ユーザ条件30」には”条件なし”が設定され、「機器条件30」には、機器が従機器であることを示す情報(”従機器”)が設定されている。すなわち、PTB-1は、コンテンツAが従機器において利用される場合にのみ選択可能となる。

【0118】

PTB-1の「価格条件30」の「ユーザ条件30」および「機器条件30」にも、実際は、図23(A)に示すように、各コードのコード値が設定されている。「ユーザ条件30」には、”条件なし”を意味する0000hのサービスコード(図15(A))が、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード(図15(B))が設定されている。「機器条件30」は、”従機器”とされているので、”機器に関し条件有り”を意味する00xxhのサービスコードが、このとき”数値100”を示す000064hのバリューコードが、そして”<(小さい)”を意味する03hのコンディションコードが設定されている。この例の場合、従機器には、100番より小さい機器番号が設定されているので、このようなコード値が設定される。

【0119】

PTB-1の「価格内容31」の”100円”は、UCPB（図12（B））の「利用内容21」の「形式21」が”Pay Per Play4”とされているので、4回の再生を行う場合の料金を示し、「価格内容32」の”300円”は、UCPBの「利用内容22」の「形式22」が”Pay Per Copy2”とされているので、2回の複製を行う場合の料金を示している。

【0120】

UCPBに対応して作成された、もう一方の図22（B）のPTB-2には、コンテンツAのID、コンテンツプロバイダ2-1のID、UCPBのID、サービスプロバイダ3-1のID、PTB-2のID、PTB-2の有効期限、価格条件40、および2通りの価格内容41、42などが含まれている。

【0121】

PTB-2の「価格条件40」の「ユーザ条件40」には”条件なし”が設定され、その「機器条件40」には、機器が主機器であることを条件とする情報（”主機器”）が設定されている。すなわち、PTB-2は、主機器においてコンテンツAが利用される場合にのみ選択可能となる。

【0122】

PTB-2の「価格条件40」の「ユーザ条件40」および「機器条件40」にも、実際は、図23（B）に示すように、各コードのコード値が設定されている。「価格条件40」の「ユーザ条件40」には、”条件なし”を意味する0000hのサービスコード（図15（A））が、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード（15（B））が設定されている。「機器条件40」には、”機器に関し条件有り”を意味する00xxhのサービスコードが、このとき”数値100”を示す000064hのバリューコードが、そして”=>（以上）”を意味する06hのコンディションコードが設定されている。

【0123】

PTB-2の「価格内容41」および「価格内容42」のそれぞれに示される価格は、UCPBの「利用内容21」の「形式21」および「利用内容22」の「形

式 2 2」のそれぞれに示される利用形式でコンテンツ A を利用する場合の料金を示している。

【0 1 2 4】

ここで、PTB - 1（従機器に適用される）の価格内容と PTB - 2（主機器に適用される）の価格内容を比較すると、PTB - 1 の価格内容は、PTB - 2 の価格内容の 2 倍に設定されている。例えば、PTB - 1 の「価格内容 3 1」が” 1 0 0 円”とされているのに対し、PTB - 2 の「価格内容 4 1」は 5 0 円とされており、「価格内容 3 2」が” 3 0 0 円”とされているのに対して、「価格内容 4 2」は” 1 5 0 円”とされている。

【0 1 2 5】

図 1 9 に戻り、ポリシー記憶部 4 3 は、コンテンツプロバイダ 2 から供給された、コンテンツの UCP を記憶し、セキュアコンテナ作成部 4 4 に供給する。

【0 1 2 6】

セキュアコンテナ作成部 4 4 は、例えば、図 2 4 に示すような、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、UCPA, B、コンテンツプロバイダ 2 の署名、PT A - 1, A - 2, B - 1, B - 2、およびサービスプロバイダ 3 の署名からなるサービスプロバイダセキュアコンテナを作成する。

【0 1 2 7】

セキュアコンテナ作成部 4 4 はまた、作成したサービスプロバイダセキュアコンテナを、図 2 5 に示すような、証明書のバージョン番号、認証局がサービスプロバイダ 3 - 1 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3 - 1 の名前、サービスプロバイダ 3 - 1 の公開鍵 K p s p、並びに署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク 5 に供給する。

【0 1 2 8】

図 1 9 に、再び戻り、相互認証部 4 5 は、コンテンツプロバイダ 2 からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロ

バイダ2と相互認証する。相互認証部45また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証するが、このサービスプロバイダ3とユーザホームネットワーク5との相互認証は、例えば、ネットワーク4が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ3は、コンテンツプロバイダ2およびユーザホームネットワーク5と相互認証を行わなくてもよい。

【0129】

サービスプロバイダ3-2の構成は、サービスプロバイダ3-1の構成と基本的に同様であるので、その図示および説明は省略する。

【0130】

次に、図26のブロック図を参照して、ユーザホームネットワーク5を構成するレシーバ51の構成例を説明する。レシーバ51は、通信部61、SAM62、外部記憶部63、伸張部64、通信部65、インタフェース66、表示制御部67、および入力制御部68より構成されている。通信部61は、ネットワーク4を介してサービスプロバイダ3、またはEMDサービスセンタ1と通信し、所定の情報を受信し、または送信する。

【0131】

SAM62は、相互認証モジュール71、課金処理モジュール72、記憶モジュール73、復号/暗号化モジュール74、およびデータ検査モジュール75からなるが、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパ性）を有している。

【0132】

SAM62の相互認証モジュール71は、記憶モジュール73に記憶されている、図27に示すSAM62の証明書を送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵Ktemp（セッション

鍵)を復号/暗号化モジュール74に供給する。SAMの証明書には、コンテンツプロバイダ2-1の証明書(図18)およびサービスプロバイダ3-1の証明書(図25)に含まれている情報に対応する情報が含まれているので、その説明は省略する。

【0133】

課金処理モジュール72は、選択されたUCPの利用内容に基づいて、UCSおよび課金情報を作成する。図28は、図12(A)に示したUCPAの利用内容11と、図20(A)に示したPTA-1に基づいて作成されたUCSAを表している。UCSには、図28に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「利用履歴」などの項目に設定される情報が含まれている。

【0134】

UCSの、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、および「PTの有効期限」の各項目には、PTの、それらに対応する項目の情報が設定される。すなわち、図28のUCSAの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3-1のIDが、「PTのID」には、PTA-1のIDが、そして「PTの有効期限」には、PTA-1の有効期限が、それぞれ設定されている。

【0135】

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSAの「UCSのID」には、UCSAのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSAの「SAMのID」には、レシーバ51のSAM62のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSAの「ユーザのID」には、ユーザFのIDが設定されている。

【0136】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」などの項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容11」の「ID11」に設定されている情報（利用内容11のID）が、「形式」には、「利用内容11」の「形式11」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容11」の「パラメータ11」に設定されている情報（”買い取り再生”に対応する情報）が設定される。

【0137】

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDと管理移動先の機器のIDは、共に、管理移動元の機器のIDとされる。一方、UCPの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には、”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われず（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容11」の「管理移動許可情報11」に”可”が設定されており、また、このとき、コンテンツAは管理移動されていないので、SAM62のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

【0138】

「利用履歴」には、同一のコンテンツに対する利用履歴が含まれている。UCSAの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ51において、コンテンツAが以前に利用されていた場合、そのときの利用形式を示す情報も記憶されている。

【0139】

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上

述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

【0140】

作成されたUCSは、レシーバ51の復号／暗号化モジュール74の復号化ユニット91から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）とともに、外部記憶部63に送信され、その利用情報記憶部63Aに記憶される。外部記憶部63の利用情報記憶部63Aは、図29に示すように、M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM62から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSは、利用情報用記憶部63Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

【0141】

図29の例では、ブロックBP-1の利用情報用メモリ領域RP-3に、図28に示したUCSAと、コンテンツAを復号するためのコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）が対応して記憶されている。ブロックBP-1の利用情報用メモリ領域RP-1、RP-2には、他のコンテンツ鍵Kco1、Kco2（それぞれ保存用鍵Ksaveで暗号化されている）およびUCS1、2がそれぞれ記憶されている。ブロックBP-1の利用情報用メモリ領域RP-4（図示せず）乃至RP-N、およびブロックBP-2（図示せず）乃至BP-Mには、コンテンツ鍵KcoおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域RPに記憶されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

【0142】

図30は、図28に示したUCSAと同時に作成された課金情報Aを表している

。課金情報には、図 30 に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「課金履歴」などの項目に設定される情報が含まれている。

【0143】

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報が、それぞれ設定されている。すなわち、図 30 の課金情報 A の、「コンテンツのID」には、コンテンツ A のIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ 2-1 のIDが、「UCPのID」には、UCPA のIDが、「UCPの有効期限」には、UCPA の有効期限が、「サービスプロバイダのID」には、サービスプロバイダ 3-1 のIDが、「PTのID」には、PTA-1 のIDが、「PTの有効期限」には、PTA-1 の有効期限が、「UCSのID」には、UCSA のIDが、「SAMのID」には、SAM 62 のIDが、「ユーザのID」には、ユーザ F のIDが、そして「利用内容」には、UCSA の「利用内容 11」の内容が、それぞれ設定されている。

【0144】

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報などが設定される。課金情報 A の「課金履歴」には、レシーバ 51 において計上された課金の合計額が設定されている。

【0145】

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらを UCS に設定しないようにすることもできる。また、上述した課金情報において、「コンテンツプロバイダのID」が設けられているが、UCP のID がユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PT のID がユニークで、これにより、サービスプロバイダ

を特定することができる場合、それを設けないようにすることもできる。

【0146】

図26に戻り、記憶モジュール73には、図31に示すように、SAM62の公開鍵K_{pu}、SAM62の秘密鍵K_{su}、EMDサービスセンタ1の公開鍵K_{pesc}、認証局の公開鍵K_{pca}、保存用鍵K_{save}、3月分の配送用鍵K_dなどの各種鍵、SAM62の証明書(図27)、課金情報(例えば、図30の課金情報Aなど)、基準情報51、およびM個の検査値HP-1乃至HP-Mなどが記憶されている。

【0147】

図32は、記憶モジュール73に記憶されている基準情報51を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定の情報などが含まれている。

【0148】

基準情報の、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の項目には、EMDサービスセンタ1のユーザ管理部18により管理されるシステム登録情報(図9)の、それらに対応する項目の情報が設定される。すなわち、基準情報51には、SAM62のID、SAM62の機器番号(100番)、ユーザFの決済ID、ユーザFの決済ユーザ情報(ユーザFのユーザ一般情報(氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別)、ユーザFのID、およびユーザFのパスワード)、および図33に示す利用ポイント情報(図10(A)に示したものと同様の情報)が設定されている。

【0149】

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる額が、課金の上限額として設定される。基準情報51の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額”正式登録時の上限額”)が設定されている。なお、正式登録されている状態における課金の上限額は、仮登録さ

れている状態における課金の上限額よりも、大きな額である。

【0150】

次に、記憶モジュール73に記憶される、図31に示したM個の検査値HP-1乃至HP-Mについて説明する。検査値HP-1は、外部記憶部63の利用情報記憶部63A（図29）のブロックBP-1に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP-2乃至HP-Mも、検査値HP-1と同様に、外部記憶部63の、対応するブロックBP-2乃至BP-Mのそれぞれに記憶されているデータのハッシュ値である。

【0151】

図26に戻り、SAM62の復号/暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、必要に応じて（例えば、相互認証時）、所定の桁数の乱数を発生して一時鍵Ktempを生成し、暗号化ユニット93に出力する。

【0152】

暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、再度、記憶モジュール73に保持されている保存用鍵Ksaveで暗号化する。暗号化されたコンテンツ鍵Kcoは、外部記憶部63に供給される。暗号化ユニット93は、コンテンツ鍵Kcoを伸張部64に送信するとき、コンテンツ鍵Kcoを乱数発生ユニット92で生成した一時鍵Ktempで暗号化する。

【0153】

データ検査モジュール75は、記憶モジュール73に記憶されている検査値HPと、外部記憶部63の利用情報記憶部63Aの、対応するブロックBPのデータのハッシュ値を比較し、ブロックBPのデータが改竄されていないか否かを検査する。データ検査モジュール75はまた、コンテンツの購入、移動、および管理移動等が行われる際に、検査値HPを再算出し、記憶モジュール73に記憶（更新）させる。

【0154】

伸張部64は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォーターマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62と相互認証し、一時鍵Ktempを復号モジュール102に出力する。復号モジュール102は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォーターマーク付加モジュール105に出力する。ウォーターマーク付加モジュール105は、コンテンツにレシーバ51を特定するための情報（例えば、SAM62のID）のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

【0155】

通信部65は、ユーザホームネットワーク5のレシーバ201との通信処理を行う。インターフェース66は、SAM62および伸張部64からの信号を所定の形式に変更し、HDD52に出力し、また、HDD52からの信号を所定の形式に変更し、SAM62および伸張部64に出力する。

【0156】

表示制御部67は、表示部（図示せず）への出力を制御する。入力制御部68は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

【0157】

HDD52は、サービスプロバイダ3から供給されたコンテンツ、UCP、およびPTの他、図34に示すような、登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

【0158】

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ51のSAM62のIDが（「対象SAMID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶さ

れ、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ51には、他の機器が接続されていないので、自分自身を含む値1が（「接続されている機器数」の欄に）記憶されている。

【0159】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件として、それぞれの項目に所定の情報が記憶されている。

【0160】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のIDが記憶されている。「ユーザID」には、対応する機器のユーザのIDが記憶される。この例の場合、ユーザFのIDが記憶されている。

【0161】

「購入処理」には、コンテンツを購入するための処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51は、コンテンツを購入するための処理を行うことができるので、“可”が記憶されている。

【0162】

「課金処理」には、EMDサービスセンタ1との間で、課金を決済する処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51は、ユーザFが決済ユーザとして登録されているので、課金を決済する処理を行うことができる。そのため、「課金処理」には、“可”が記憶されている。

【0163】

「課金機器」には、計上された課金に対する課金処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ51（SAM62）は、自分自身が、課金を決済することができるので、SAM62のIDが記憶されている。

【0164】

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ3からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ51は、コンテンツの供給をサービスプロバイダ3から受けるので、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。

【0165】

「状態フラグ」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、決済が成功しなかった場合や、正式登録されるための与信処理が完了していない場合（仮登録されている場合）、「状態フラグ」には、”制限あり”が設定される。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツを利用する処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

【0166】

この例の場合、レシーバ51に対しては、何ら制限が課せられていないものとし、「状態フラグ」には”なし”が設定されている。

【0167】

「登録条件署名」には、登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。この例の場合、レシーバ51の登録条件に対する署名が記憶されている。「登録リスト署名」には、登録リストに設定されたデータの全体に対する署名が設定されている。

【0168】

図 35 は、レシーバ 201 の構成例を表している。レシーバ 201 の通信部 211 乃至入力制御部 218 は、レシーバ 51 の通信部 61 乃至入力制御部 68 と同様の機能を有しているので、その説明は適宜省略する。

【0169】

SAM 212 の記憶モジュール 223 にも、図 36 に示すように、SAM 212 の公開鍵 K_{pu} 、SAM 212 の秘密鍵 K_{su} 、EMD サービスセンタ 1 の公開鍵 K_{pes} 、認証局の公開鍵 K_{pca} 、保存用鍵 K_{save} 、3 月分の配送用鍵 K_d 、予め認証局から配布されている SAM 212 の証明書、および基準情報 201 が記憶されている。基準情報 201 には、図 37 に示すように、SAM 212 の ID、レシーバ 201 の機器番号 (100 番)、ユーザ A の決済 ID、ユーザ A の決済ユーザ情報 (ユーザ A のユーザ一般情報 (氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別)、ユーザ A の ID、およびユーザ A のパスワード)、および図 38 に示す利用ポイント情報 (図 10 (B) に示したものと同様の情報) が設定されている。

【0170】

HDD 202 は、HDD 52 と同様の機能を有するので、その説明は省略する。

【0171】

次に、EMD システムの処理について、図 39 のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ 2-1 に保持されているコンテンツ A が、サービスプロバイダ 3-1 を介して、ユーザホームネットワーク 5 のレシーバ 51 に供給され、利用される場合を例として説明する。

【0172】

ステップ S11 において、配送用鍵 K_d が、EMD サービスセンタ 1 からコンテンツプロバイダ 2-1 に供給される処理が行われる。この処理の詳細は、図 40 のフローチャートに示されている。すなわち、ステップ S31 において、EMD サービスセンタ 1 の相互認証部 17 は、コンテンツプロバイダ 2-1 の相互認証部 39 と相互認証し、コンテンツプロバイダ 2-1 が、正当なプロバイダであることが確認した後、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 12 は、鍵サーバ 14 から供給された配送用鍵 K_d をコンテンツプロバイダ 2-1 に送信

する。なお、相互認証処理の詳細は、図4 1乃至図4 3を参照して後述する。

【0173】

次に、ステップS 3 2において、コンテンツプロバイダ2-1の暗号化部3 6は、EMDサービスセンタ1から送信された配送用鍵K dを受信し、ステップS 3 3において、記憶する。

【0174】

このように、コンテンツプロバイダ2-1の暗号化部3 6が、配送用鍵K dを記憶したとき、処理は終了し、図3 9のステップS 1 2に進む。ここで、ステップS 1 2以降の処理の説明の前に、図4 0のステップS 3 1における相互認証処理（なりすましがないことを確認する処理）について、1つの共通鍵を用いる場合（図4 1）、2つの共通鍵を用いる場合（図4 2）、および公開鍵暗号を用いる場合（図4 3）を例として説明する。

【0175】

図4 1は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部3 9とEMDサービスセンタ1の相互認証部1 7との相互認証の動作を説明するフローチャートである。ステップS 4 1において、コンテンツプロバイダ2の相互認証部3 9は、64ビットの乱数R 1を生成する（乱数生成部3 5が生成するようにしてもよい）。ステップS 4 2において、コンテンツプロバイダ2の相互認証部3 9は、DESを用いて乱数R 1を、予め記憶している共通鍵K cで暗号化する（暗号化部3 6で暗号化するようにしてもよい）。ステップS 4 3において、コンテンツプロバイダ2の相互認証部3 9は、暗号化された乱数R 1をEMDサービスセンタ1の相互認証部1 7に送信する。

【0176】

ステップS 4 4において、EMDサービスセンタ1の相互認証部1 7は、受信した乱数R 1を予め記憶している共通鍵K cで復号する。ステップS 4 5において、EMDサービスセンタ1の相互認証部1 7は、32ビットの乱数R 2を生成する。ステップS 4 6において、EMDサービスセンタ1の相互認証部1 7は、復号した64ビットの乱数R 1の下位32ビットを乱数R 2で入れ替え、接続 $R 1_H \parallel R 2$ を生成する。なお、ここで $R i_H$ は、 $R i$ の上位ビットを表し、 $A \parallel B$ は、

AとBの接続（ n ビットのAの下位に、 m ビットのBを結合して、 $(n+m)$ ビットとしたもの）を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いて $R1_H \parallel R2$ を共通鍵 Kc で暗号化する。ステップS48において、EMDサービスセンタ1の相互認証部17は、暗号化した $R1_H \parallel R2$ をコンテンツプロバイダ2に送信する。

【0177】

ステップS49において、コンテンツプロバイダ2の相互認証部39は、受信した $R1_H \parallel R2$ を共通鍵 Kc で復号する。ステップS50において、コンテンツプロバイダ2の相互認証部39は、復号した $R1_H \parallel R2$ の上位32ビット $R1_H$ を調べ、ステップS41で生成した、乱数 $R1$ の上位32ビット $R1_H$ と一致すれば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数 $R1_H$ と、受信した $R1_H$ が一致しないとき、処理は終了される。両者が一致するとき、ステップS51において、コンテンツプロバイダ2の相互認証部39は、32ビットの乱数 $R3$ を生成する。ステップS52において、コンテンツプロバイダ2の相互認証部39は、受信し、復号した32ビットの乱数 $R2$ を上位に設定し、生成した乱数 $R3$ をその下位に設定し、接続 $R2 \parallel R3$ とする。ステップS53において、コンテンツプロバイダ2の相互認証部39は、DESを用いて接続 $R2 \parallel R3$ を共通鍵 Kc で暗号化する。ステップS54において、コンテンツプロバイダ2の相互認証部39は、暗号化された接続 $R2 \parallel R3$ をEMDサービスセンタ1の相互認証部17に送信する。

【0178】

ステップS55において、EMDサービスセンタ1の相互認証部17は、受信した接続 $R2 \parallel R3$ を共通鍵 Kc で復号する。ステップS56において、EMDサービスセンタ1の相互認証部17は、復号した接続 $R2 \parallel R3$ の上位32ビットを調べ、乱数 $R2$ と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【0179】

図42は、2つの共通鍵 $Kc1$ 、 $Kc2$ で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部

17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を予め記憶している共通鍵Kc1で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1に送信する。

【0180】

ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kc1で復号する。ステップS65において、EMDサービスセンタ1の相互認証部17は、乱数R1を予め記憶している共通鍵Kc2で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数R2を共通鍵Kc2で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数R1および乱数R2をコンテンツプロバイダ2の相互認証部39に送信する。

【0181】

ステップS69において、コンテンツプロバイダ2の相互認証部39は、受信した乱数R1および乱数R2を予め記憶している共通鍵Kc2で復号する。ステップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数R1を調べ、ステップS61で生成した乱数R1（暗号化する前の乱数R1）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS71において、コンテンツプロバイダ2の相互認証部39は、復号して得た乱数R2を共通鍵Kc1で暗号化する。ステップS72において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R2をEMDサービスセンタ1に送信する。

【0182】

ステップS73において、EMDサービスセンタ1の相互認証部17は、受信した乱数R2を共通鍵Kc1で復号する。ステップS74において、EMDサービス

センタ 1 の相互認証部 17 は、復号した乱数 R_2 が、ステップ S 66 で生成した乱数 R_2 （暗号化する前の乱数 R_2 ）と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【0183】

図 43 は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ S 81 において、コンテンツプロバイダ 2 の相互認証部 39 は、64ビットの乱数 R_1 を生成する。ステップ S 82 において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵 K_{pcp} を含む証明書（認証局から予め取得しておいたもの）と、乱数 R_1 を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0184】

ステップ S 83 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した証明書の署名（認証局の秘密鍵 K_{sca} で暗号化されている）を、予め取得しておいた認証局の公開鍵 K_{pca} で復号し、コンテンツプロバイダ 2 の公開鍵 K_{pcp} とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 K_{pcp} が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【0185】

適正な認証結果が得られたとき、ステップ S 84 において、EMD サービスセン

タ 1 の相互認証部 17 は、64 ビットの乱数 R_2 を生成する。ステップ S 85 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R_1 および乱数 R_2 の接続 $R_1 \parallel R_2$ を生成する。ステップ S 86 において、EMD サービスセンタ 1 の相互認証部 17 は、接続 $R_1 \parallel R_2$ を自分自身の秘密鍵 $K_{se sc}$ で暗号化する。ステップ S 87 において、EMD サービスセンタ 1 の相互認証部 17 は、接続 $R_1 \parallel R_2$ を、ステップ S 83 で取得したコンテンツプロバイダ 2 の公開鍵 $K_{pc p}$ で暗号化する。ステップ S 88 において、EMD サービスセンタ 1 の相互認証部 17 は、秘密鍵 $K_{se sc}$ で暗号化された接続 $R_1 \parallel R_2$ 、公開鍵 $K_{pc p}$ で暗号化された接続 $R_1 \parallel R_2$ 、および自分自身の公開鍵 $K_{pe sc}$ を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

【0186】

ステップ S 89 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 $K_{pc a}$ で復号し、正しければ証明書から公開鍵 $K_{pe sc}$ を取り出す。この場合の処理は、ステップ S 83 における場合と同様であるので、その説明は省略する。ステップ S 90 において、コンテンツプロバイダ 2 の相互認証部 39 は、EMD サービスセンタ 1 の秘密鍵 $K_{se sc}$ で暗号化されている接続 $R_1 \parallel R_2$ を、ステップ S 89 で取得した公開鍵 $K_{pe sc}$ で復号する。ステップ S 91 において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵 $K_{pc p}$ で暗号化されている接続 $R_1 \parallel R_2$ を、自分自身の秘密鍵 $K_{sc p}$ で復号する。ステップ S 92 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 90 で復号された接続 $R_1 \parallel R_2$ と、ステップ S 91 で復号された接続 $R_1 \parallel R_2$ を比較し、一致すれば EMD サービスセンタ 1 を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【0187】

適正な認証結果が得られたとき、ステップ S 93 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 R_3 を生成する。ステップ S 94 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 90 で取得

した乱数 R_2 および生成した乱数 R_3 の接続 $R_2 \parallel R_3$ を生成する。ステップ S 95 において、コンテンツプロバイダ 2 の相互認証部 39 は、接続 $R_2 \parallel R_3$ を、ステップ S 89 で取得した公開鍵 K_{pesc} で暗号化する。ステップ S 96 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化した接続 $R_2 \parallel R_3$ を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0188】

ステップ S 97 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された接続 $R_2 \parallel R_3$ を自分自身の秘密鍵 K_{sesc} で復号する。ステップ S 98 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した乱数 R_2 が、ステップ S 84 で生成した乱数 R_2 (暗号化する前の乱数 R_2) と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【0189】

以上のように、EMD サービスセンタ 1 の相互認証部 17 とコンテンツプロバイダ 2 の相互認証部 39 は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵 K_{temp} として利用される。

【0190】

次に、図 39 のステップ S 12 の処理について説明する。ステップ S 12 においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ 2-1 からサービスプロバイダ 3-1 に供給される処理が行われる。その処理の詳細は、図 44 のフローチャートに示されている。すなわち、ステップ S 201 において、コンテンツプロバイダ 2-1 のウォーターマーク付加部 32 は、コンテンツサーバ 31 からコンテンツ A を読み出し、コンテンツプロバイダ 2-1 を示す所定のウォーターマーク (電子透かし) を挿入し、圧縮部 33 に供給する。

【0191】

ステップ S 202 において、コンテンツプロバイダ 2-1 の圧縮部 33 は、ウォーターマークが挿入されたコンテンツ A を ATRAC2 等の所定の方式で圧縮し、暗号化部 34 に供給する。ステップ S 203 において、乱数発生部 35 は、コンテンツ鍵 K_{coA} となる乱数を発生させ、暗号化部 34 に供給する。

【0192】

ステップS204において、コンテンツプロバイダ2-1の暗号化部34は、DESなどの所定の方式で、乱数発生部35で発生された乱数（コンテンツ鍵Kc o A）を使用して、ウォーターマークが挿入されて圧縮されたコンテンツAを暗号化する。次に、ステップS205において、暗号化部36は、DESなどの所定の方式で、EMDサービスセンタ1から供給された配送用鍵Kdでコンテンツ鍵Kc o Aを暗号化する。

【0193】

ステップS206において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵Kc o Aで暗号化されている）、コンテンツ鍵Kc o A（配送用鍵Kdで暗号化されている）、およびポリシー記憶部37に記憶されている、コンテンツAに対応するUCPA, B（図12）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ksc pで暗号化する。これにより、図17に示した署名が作成される。

【0194】

ステップS207において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵Kc o Aで暗号化されている）、コンテンツ鍵Kc o A（配送用鍵Kdで暗号化されている）、UCPA, B（図12）、およびステップS206で生成した署名を含んだ、図17に示したコンテンツプロバイダセキュアコンテナを作成する。

【0195】

ステップS208において、コンテンツプロバイダ2-1の相互認証部39は、サービスプロバイダ3-1の相互認証部45と相互認証する。この認証処理は、図41乃至図43を参照して説明した場合と同様であるので、その説明は省略する。ステップS209において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、認証局から予め発行された証明書（図18）を、ステップS207で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ3-1に送信する。

【0196】

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ3-1に供給されたとき、処理は終了し、図39のステップS13に進む。

【0197】

ステップS13において、サービスプロバイダセキュアコンテナが、サービスプロバイダ3-1からユーザホームネットワーク5（レシーバ51）に供給される。この処理の詳細は、図45のフローチャートに示されている。すなわち、ステップS221において、サービスプロバイダ3-1の値付け部42は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図18）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ2-1の公開鍵K_{pcp}を取り出す。証明書の署名の確認は、図43のステップS83における処理と同様であるので、その説明は省略する。

【0198】

ステップS222において、サービスプロバイダ3-1の値付け部42は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2-1の公開鍵K_{pcp}で復号し、得られたハッシュ値が、コンテンツA（コンテンツ鍵K_{coA}で暗号化されている）、コンテンツ鍵K_{coA}（配送用鍵K_dで暗号化されている）、およびUCPA、Bの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップS223に進む。

【0199】

ステップS223において、サービスプロバイダ3-1の値付け部42は、コンテンツプロバイダセキュアコンテナから、コンテンツA（コンテンツ鍵K_{coA}で暗号化されている）、コンテンツ鍵K_{coA}（配送用鍵K_dで暗号化されている）、および署名を取り出し、コンテンツサーバ41に供給する。コンテンツサーバ41は、それらを記憶する。値付け部42はまたUCPA、Bも、コンテン

ツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部 44 に供給する。

【0200】

ステップ S224 において、サービスプロバイダ 3-1 の値付け部 42 は、取り出した UCPA, B に基づいて、PTA-1, A-2 (図 20)、および PTB-1, B-2 (図 22) を作成し、セキュアコンテナ作成部 44 に供給する。

【0201】

ステップ S225 において、サービスプロバイダ 3-1 のセキュアコンテナ作成部 44 は、コンテンツサーバ 41 から読み出したコンテンツ A (コンテンツ鍵 KcoA で暗号化されている)、コンテンツ鍵 KcoA (配送用鍵 Kd で暗号化されている)、およびコンテンツプロバイダ 2 の署名、値付け部 42 から供給された、UCPA, B、および PTA-1, A-2, B-1, B-2、並びにその署名から、図 24 に示したサービスプロバイダセキュアコンテナを作成する。

【0202】

ステップ S226 において、サービスプロバイダ 3-1 の相互認証部 45 は、レシーバ 51 の相互認証モジュール 71 と相互認証する。この認証処理は、図 41 乃至図 43 を参照して説明した場合と同様であるので、その説明を省略する。

【0203】

ステップ S227 において、サービスプロバイダ 3-1 のセキュアコンテナ作成部 44 は、ステップ S225 で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ 3-1 の証明書 (図 25) を付して、ユーザホームネットワーク 5 のレシーバ 51 に送信する。

【0204】

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ 3-1 からレシーバ 51 に送信されたとき、処理は終了し、図 39 のステップ S14 に進む。

【0205】

ステップ S14 において、サービスプロバイダ 3-1 から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク 5 のレシーバ 51 に

より受信される。この処理の詳細は、図46のフローチャートに示されている。すなわち、ステップS241において、レシーバ51の相互認証モジュール71は、通信部61を介して、サービスプロバイダ3-1の相互認証部45と相互認証し、相互認証できたとき、通信部61は、相互認証したサービスプロバイダ3-1から、サービスプロバイダセキュアコンテナ（図24）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップS242に進む。

【0206】

ステップS242において、レシーバ51の通信部61は、ステップS241で相互認証したサービスプロバイダ3-1から、公開鍵証明書を受信する。

【0207】

ステップS243において、レシーバ51の復号/暗号化モジュール74は、ステップS241で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップS244に進む。

【0208】

ステップS244において、UCPおよびPTが選択され、かつ、その利用内容および価格内容が選択される。具体的には、レシーバ51の記憶モジュール73に記憶されている基準情報51（図32）が、利用条件を満たすUCPと価格条件を満たすPTが選択される。この例の場合、レシーバ51の基準情報51の「利用ポイント情報」には、図33に示したように、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイントであるとされている。すなわち、この基準情報51によれば、コンテンツAに対応して設定されたUCPA、Bのうち、「利用条件10」の「ユーザ条件10」が”200ポイント以上”とされているUCPA（図12（A））が選択される。また、基準情報51の「決済ユーザ情報」には、ユーザFは男性とされているので、PTA-1（図20（A））の「価格条件10」に設定された条件を満たす。その結果、UCPAに対応して作成されたPTA-1、PTA-2のうち、PTA-1が選択される。

【0209】

その後、このようにして選択されたUCPAおよびPTA-1の内容が、表示制御部67を介して、図示せぬ表示部に表示される。そこで、ユーザFは、その表示を参照して（例えば、利用したい利用形式と、その価格を比較検討して）、UCPAの所定の「利用内容」を選択するための操作を、図示せず操作部に対して行う。これにより、入力制御部68を介して、選択されたUCPAの利用内容のIDおよびPTA-1のIDがSAM62に出力される。なお、この例の場合、UCPAの利用内容11（PTA-1の価格内容11）が選択されたものとする。

【0210】

ステップS245において、レシーバ51のSAM62の課金処理モジュール72は、ステップS244で選択された、UCPAの「利用内容11」とPTA-1に基づいて、UCSA（図28）および課金情報A（図30）を作成する。すなわち、この場合、コンテンツAは、料金が2000円で買い取り再生される。

【0211】

ステップS246において、サービスプロバイダセキュアコンテナ（図24）に含まれる、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、UCPA、PTA-1、A-2、およびコンテンツプロバイダ2の署名が取り出され、HD D52に出力され、記憶される。ステップS247において、復号／暗号化ユニット74の復号ユニット91は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）を、記憶モジュール73に記憶されている配送用鍵Kdで復号する。

【0212】

ステップS248において、復号／暗号化ユニット74の暗号化ユニット93は、ステップS247で復号されたコンテンツ鍵KcoAを、記憶モジュール73に記憶されている保存用鍵Ksaveで暗号化する。

【0213】

ステップS249において、レシーバ51のデータ検査モジュール75は、ステップS248で保存用鍵Ksaveで暗号化されたコンテンツ鍵KcoA、およびステップS245で作成されたUCSAが対応して記憶される、外部記憶部6

3の利用情報記憶部63A(図29)のブロックBPを検出する。この例の場合、利用情報記憶部63AのブロックBP-1が検出される。なお、図29の利用情報記憶部63Aにおいて、そのブロックBP-1の利用情報用メモリ領域RP-3にコンテンツ鍵KcoAおよびUCSAが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、空いることを示す所定の初期情報が記憶されている。

【0214】

ステップS250において、レシーバ51のデータ検査モジュール75は、ステップS249で検出したブロックBP-1のデータ(利用情報用メモリ領域RP-1乃至RP-Nに記憶されている全てのデータ)にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップS251において、データ検査モジュール75は、ステップS250で得られたハッシュ値と、記憶モジュール73に記憶されているブロックBP-1に対応する検査値HP-1(図31)とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックBP-1のデータは改竄されていないので、ステップS252に進む。

【0215】

ステップS252において、レシーバ51のSAM62は、利用情報(ステップS248で、保存用鍵Ksaveで暗号化されたコンテンツ鍵KcoA、およびステップS245で作成されたUCSA)を、外部記憶部63のブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。

【0216】

ステップS253において、レシーバ51のデータ検査モジュール75は、ステップS252で利用情報が記憶された利用情報用メモリ領域RP-3が属する、利用情報記憶部63AのブロックBP-1に記憶されている全てのデータにハッシュ関数を適用してハッシュ値を算出し、ステップS254において、記憶モジュール73に記憶されている検査値HP-1に上書きする。ステップS255において、課金処理モジュール72は、ステップS245で作成した課金情報Aを記憶モジュール73に記憶させ、処理は終了する。

【0217】

ステップ S 2 5 1 において、算出されたハッシュ値と検査値 HP-1 とが一致しないと判定された場合、ブロック BP-1 のデータは改竄されているので、手続きは、ステップ S 2 5 6 に進み、データ検査モジュール 7 5 は、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック BP を調べたか否かを判定し、外部記憶部 6 3 の全てのブロック BP を調べていないと判定した場合、ステップ S 2 5 7 に進み、利用情報記憶部 6 3 A の、空きを有する他のブロック BP を検索し、ステップ S 2 5 0 に戻り、それ以降の処理が実行される。

【0218】

ステップ S 2 5 6 において、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック BP が調べられたと判定された場合、利用情報を記憶できるブロック BP (利用情報用メモリ領域 RP) は存在しないので、処理は終了する。

【0219】

このように、サービスプロバイダセキュアコンテナが、レシーバ 5 1 により受信されると、処理は終了し、図 3 9 のステップ S 1 5 に進む。

【0220】

ステップ S 1 5 において、供給されたコンテンツ A が、レシーバ 5 1 において利用される。なお、この例の場合選択された UCPA の利用内容 1 1 によれば、コンテンツ A は、再生して利用される。そこで、ここでは、コンテンツ A の再生処理について説明する。この再生処理の詳細は、図 4 7 のフローチャートに示されている。

【0221】

ステップ S 2 6 1 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、図 4 6 のステップ S 2 5 2 で、コンテンツ鍵 K c o A (保存用鍵 K s a v e で暗号化されている) および UCSA が記憶された利用情報用メモリ領域 RP-3 が属する、外部記憶部 6 3 の利用情報記憶部 6 3 A のブロック BP-1 のデータにハッシュ関数を適用してハッシュ値を算出する。

【0222】

ステップ S 2 6 2 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、ステップ S 2 6 1 において算出したハッシュ値が、図 4 6 のステップ S 2 5 3 で算

出し、ステップ S 2 5 4 で記憶モジュール 7 3 に記憶させたハッシュ値（検査値 HP-1）と一致するか否かを判定し、一致すると判定した場合、ブロック BP-1 のデータは改竄されていないので、ステップ S 2 6 3 に進む。

【0223】

ステップ S 2 6 3 において、UCSA（図 2 8）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツ A が利用可能か否かが判定される。例えば、「利用内容」の「形式」が、「期間制限再生」とされている UCS においては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。現在の時刻がその範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされている UCS においては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が 0 回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が 0 回であるとき、利用不可と判定される。

【0224】

なお、UCSA の「利用内容」の「形式」は、「買い取り再生」とされているので、この場合、コンテンツ A は、買い取られ、制限なしに再生される。すなわち、UCSA の「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップ S 2 6 3 において、コンテンツ A が利用可能であると判定され、ステップ S 2 6 4 に進む。

【0225】

ステップ S 2 6 4 において、レシーバ 5 1 の課金モジュール 7 2 は、UCSA を更新する。UCSA には、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が 1 つだけデクリメントされる。

【0226】

次に、ステップS265において、レシーバ51のSAM62は、ステップS264で更新されたUCSA（実際は、更新されていない）を、外部記憶部63の利用情報記憶部63AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS266において、データ検査モジュール75は、ステップS265でUCSAが記憶された、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール73に記憶されている検査値HP-1に上書きする。

【0227】

ステップS267において、SAM62の相互認証モジュール71と、伸張部64の相互認証モジュール101は、相互認証し、SAM62および伸張部64は、一時鍵Ktempを共有する。この認証処理は、図41乃至図43を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、R3、またはその組み合わせが、一時鍵Ktempとして用いられる。

【0228】

ステップS268において、復号／暗号化モジュール74の復号ユニット91は、図46のステップS252で外部記憶部63の利用情報記憶部63AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されたコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）を、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。

【0229】

次に、ステップS269において、復号／暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵KcoAを一時鍵Ktempで暗号化する。ステップS270において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵KcoAを伸張部64に送信する。

【0230】

ステップS271において、伸張部64の復号モジュール102は、コンテンツ鍵KcoAを一時鍵Ktempで復号する。ステップS272において、伸張

部 64 は、インタフェース 66 を介して、HDD 52 に記録されたコンテンツ A（コンテンツ鍵 Kc o で暗号化されている）を受け取る。ステップ S 273 において、伸張部 64 の復号モジュール 103 は、コンテンツ A（コンテンツ鍵 Kc o で暗号化されている）をコンテンツ鍵 Kc o A で復号する。

【0231】

ステップ S 274 において、伸張部 64 の伸張モジュール 104 は、復号されたコンテンツ A を ATRAC2 などの所定の方式で伸張する。ステップ S 275 において、伸張部 64 のウォータマーク付加モジュール 105 は、伸張されたコンテンツ A にレシーバ 51 を特定する所定のウォータマーク（電子透かし）を挿入する。ステップ S 276 において、コンテンツ A は、図示せぬスピーカなどに出力され、再生される。その後、処理は終了する。

【0232】

ステップ S 262 において、ステップ S 261 において算出されたハッシュ値が、レシーバ 51 の記憶モジュール 73 に記憶された検査値 HP-1 と一致しないと判定された場合、またはステップ S 263 において、コンテンツが利用不可と判定された場合、ステップ S 277 において、SAM 62 は、表示制御部 67 を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【0233】

このようにして、レシーバ 51 において、コンテンツ A が再生（利用）されたとき、処理は終了し、図 39 の処理も終了する。

【0234】

なお、以上においては、コンテンツ A が、レシーバ 51 において利用（購入）される場合を例として説明したが、レシーバ 201 も、レシーバ 51 と同様に、コンテンツ A を利用することができる。ただし、レシーバ 201 の基準情報 201 の「利用ポイント情報」には、図 38 に示したように、コンテンツプロバイダ 2-1 のコンテンツ利用ポイントが 23 ポイントとされているので、UCPA の「利用条件 10」の「ユーザ条件 10」の条件を満たさない。すなわち、この場合、UCPA は選択されず、UCPB が選択される。

【0235】

次に、PTが選択されるが、この場合、UCPBが選択されているので、UCPBに対応するPTB-1, B-2 (図22) のうちのいずれかが選択される。PTB-1の「価格条件30」は、機器が従機器であることが条件とされ、またPTB-2の「価格条件40」は、主機器であることが条件とされている。すなわち、主機器であるレシーバ201においては、PTB-2が選択される。このように、機器およびそのユーザに設定された各種条件に基づいて、UCP、UCPの利用内容、およびPTの選択範囲が決定される。

【0236】

また、以上においては、UCPの「利用条件」またはPTの「価格条件」の「ユーザ条件」を、ユーザの性別や年齢に関する条件とする場合を例として説明したが、例えば、ユーザの住んでいる地域や誕生日などを条件とすることもできる。なお、この場合、図15(A)のサービスコードの0300h乃至7FFFhのコード値に、それらの条件の意味を設定する。

【0237】

次に、レシーバ51の課金が決済される場合の処理手順を、図48のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額(正式登録時の上限額または仮登録時の上限額)を超えた場合、または配送用鍵Kdのバージョンが古くなり、例えば、図46のステップS247で、コンテンツ鍵Kco(配送用鍵Kdで暗号化されている)を復号することができなくなった場合(サービスプロバイダセキュアコンテナを受信することができなくなった場合)に開始される。

【0238】

すなわち、ステップS301において、レシーバ51とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図41乃至図43を参照して説明した場合と同様の処理であるので、その説明は省略する。

【0239】

次に、ステップS302において、レシーバ51のSAM62は、EMDサービスセンタ1のユーザ管理部18に証明書を送信する。ステップS303において、レ

シーバ51のSAM62は、記憶モジュール73に記憶されている課金情報を、ステップS301でEMDサービスセンタ1と共有した一時鍵Ktempで暗号化し、配送用鍵Kdのバージョン、HDD52に記憶されているUCPおよびPT、並びに登録リストとともに、EMDサービスセンタ1に送信する。

【0240】

ステップS304において、EMDサービスセンタ1のユーザ管理部18は、ステップS303で、レシーバ51から送信された情報を受信し、復号した後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ51において存在するか否かを確認する。

【0241】

ステップS305において、EMDサービスセンタ1の課金請求部19は、ステップS303で受信された課金情報を解析し、ユーザ（例えば、ユーザF）の支払い金額を算出する処理等を行う。次に、ステップS306において、ユーザ管理部18は、ステップS305における処理により、決済が成功したか否かを確認する。

【0242】

次に、ステップS307において、EMDサービスセンタ1のユーザ管理部18は、ステップS304における確認結果、およびステップS306における確認結果に基づいて、レシーバ51の登録条件を設定し、それに署名を付して、レシーバ51の登録リストを作成する。

【0243】

例えば、ステップS304で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップS306で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

【0244】

次に、ステップ S 3 0 8 に進み、EMD サービスセンタ 1 のユーザ管理部 1 8 は、最新バージョンの配送用鍵 K d （3 月分の最新バージョンの配送用鍵 K d ）を一時鍵 K t e m p で暗号化し、ステップ S 3 0 7 で作成された登録リストとともにレシーバ 5 1 に送信する。

【0 2 4 5】

ステップ S 3 0 9 において、レシーバ 5 1 の SAM 6 2 は、EMD サービスセンタ 1 から送信された配送用鍵 K d および登録リストを、通信部 6 1 を介して受信し、復号した後、記憶モジュール 7 3 に記憶させる。このとき、記憶モジュール 7 3 に記憶されていた課金情報は消去され、登録リストおよび配送用鍵 K d が更新される。

【0 2 4 6】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0 2 4 7】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0 2 4 8】

【発明の効果】

請求項 1 に記載の情報処理装置、請求項 3 に記載の情報処理方法、および請求項 4 に記載の提供媒体によれば、第 1 の情報に対応させて、利用条件および利用内容を含む第 2 の情報を記憶するようにしたので、第 1 の情報に対応させて第 2 の情報を所定のプロバイダに送信することができる。

【0 2 4 9】

請求項 4 に記載の情報処理装置、請求項 5 に記載の情報処理方法、および請求項 6 に記載の提供媒体によれば、第 1 の情報の利用条件および利用内容を含む第 2 の情報に対応して、第 1 の情報の価格条件および価格内容を含む第 3 の情報を作成するようにしたので、第 1 の情報に対応させて第 2 の情報および第 3 の情報を、所定の機器に送信することができる。

【0250】

請求項7に記載の情報処理装置、請求項8に記載の情報処理方法、および請求項9に記載の提供媒体によれば、基準情報に対応して選択した利用条件に対応する利用内容に従って、コンテンツを利用し、基準情報に対応して選択した価格条件に対応する価格内容に従って、コンテンツの利用に対して、課金処理を実行するようにしたので、変化に富んだサービスを受けることができる。

【図面の簡単な説明】

【図1】

EMDシステムを説明する図である。

【図2】

EMDシステムにおける、主な情報の流れを説明する図である。

【図3】

EMDサービスセンタ1の機能的構成を示すブロック図である。

【図4】

EMDサービスセンタ1の配送用鍵K dの送信を説明する図である。

【図5】

EMDサービスセンタ1の配送用鍵K dの送信を説明する他の図である。

【図6】

EMDサービスセンタ1の配送用鍵K dの送信を説明する他の図である。

【図7】

EMDサービスセンタ1の配送用鍵K dの送信を説明する他の図である。

【図8】

EMDサービスセンタ1の配送用鍵K dの送信を説明する他の図である。

【図9】

システム登録情報を説明する図である。

【図10】

利用ポイント情報を説明する図である。

【図11】

コンテンツプロバイダ2の機能的構成例を示すブロック図である。

【図 1 2】

UCPの例を示す図である。

【図 1 3】

コンテンツの管理移動を説明する図である。

【図 1 4】

第 1 世代複製を説明する図である。

【図 1 5】

サービスコードおよびコンディションコードのコード値の例を示す図である。

【図 1 6】

UCPの利用条件として設定されたコード値の例を示す図である。

【図 1 7】

コンテンツプロバイダセキュアコンテナの例を示す図である。

【図 1 8】

コンテンツプロバイダ 2 の証明書の例を示す図である。

【図 1 9】

サービスプロバイダ 3 の機能的構成を示すブロック図である。

【図 2 0】

PTの例を示す図である。

【図 2 1】

PTの価格条件として設定されたコード値の例を示す図である。

【図 2 2】

他のPTの例を示す図である。

【図 2 3】

他のPTの価格条件として設定されたコード値の例を示す図である。

【図 2 4】

サービスプロバイダセキュアコンテナの例を示す図である。

【図 2 5】

サービスプロバイダ 3 の証明書の例を示す図である。

【図 2 6】

ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック図である。

【図 2 7】

レシーバ 5 1 の SAM 6 2 の証明書の例を示す図である。

【図 2 8】

UCS の例を示す図である。

【図 2 9】

レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する図である。

【図 3 0】

課金情報の例を示す図である。

【図 3 1】

レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図である。

【図 3 2】

基準情報 5 1 を説明する図である。

【図 3 3】

基準情報 5 1 の利用ポイント情報の例を示す図である。

【図 3 4】

登録リストの例を示す図である。

【図 3 5】

ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示すブロック図である。

【図 3 6】

レシーバ 2 0 1 の記憶モジュール 2 2 3 に記憶されている情報の例を示す図である。

【図 3 7】

基準情報 2 0 1 の例を示す図である。

【図 3 8】

基準情報 5 1 の利用ポイント情報の例を示す図である。

【図 3 9】

コンテンツの利用処理を説明するフローチャートである。

【図 4 0】

EMDサービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

【図 4 1】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 4 2】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 4 3】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 4 4】

コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 4 5】

サービスプロバイダ 3 がレシーバ 5 1 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 4 6】

レシーバ 5 1 がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

【図 4 7】

レシーバ 5 1 がコンテンツを再生する処理を説明するフローチャートである。

【図 4 8】

決済処理を説明するフローチャートである。

【符号の説明】

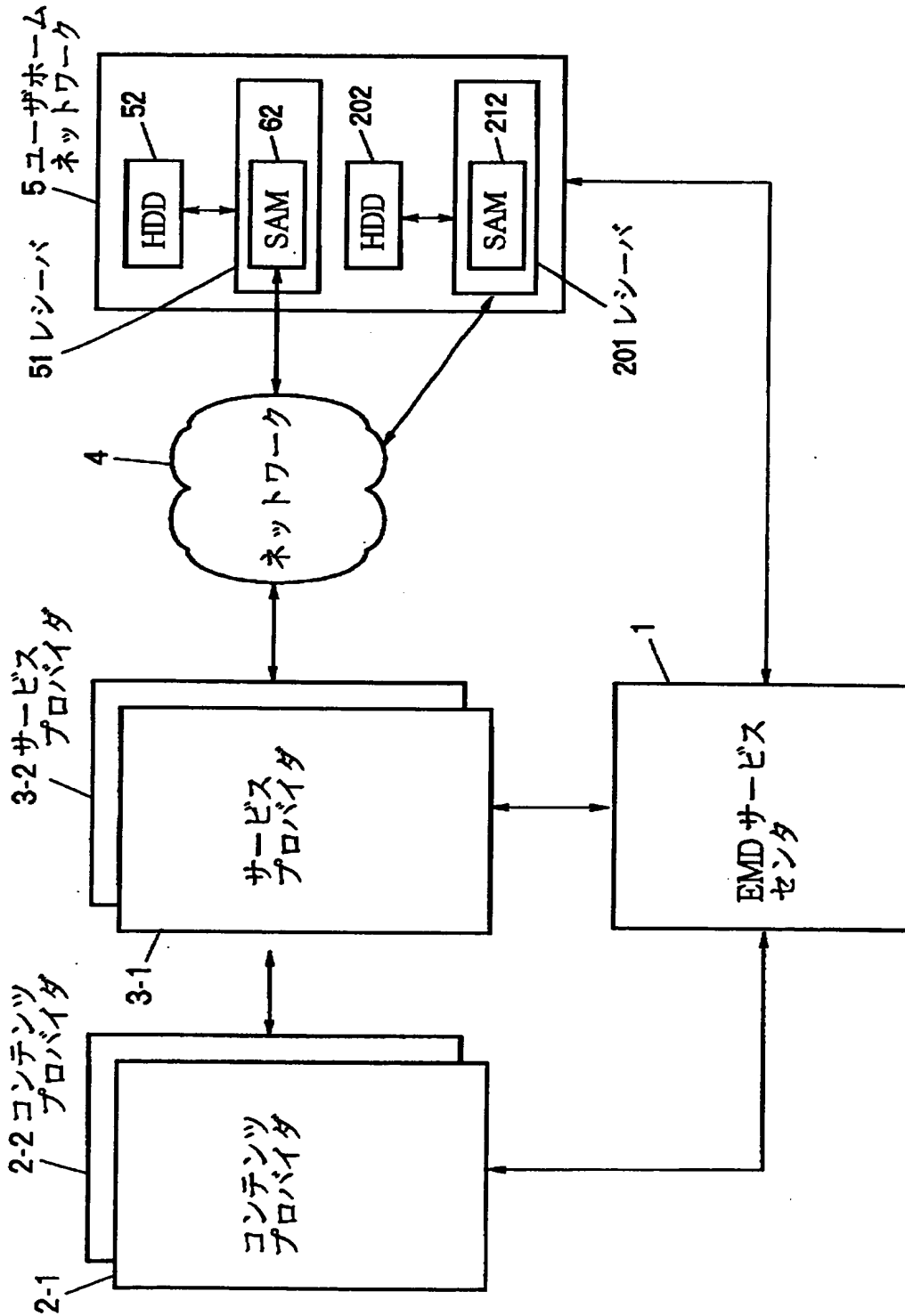
1 EMDサービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロ

バイダ, 5 ユーザホームネットワーク, 11 サービスプロバイダ管理部,
 12 コンテンツプロバイダ管理部, 13 著作権管理部, 14 鍵サ
 ーバ, 15 経歴データ管理部, 16 利益分配部, 17 相互認証部,
 18 ユーザ管理部, 19 課金請求部, 20 出納部, 21 監査部,
 31 コンテンツサーバ, 32 ウォータマーク付加部, 33 圧縮部,
 34 暗号化部, 35 乱数発生部, 36 暗号化部, 37 ポリシ
 ー記憶部, 38 セキュアコンテナ作成部, 39 相互認証部, 41 コ
 ンテンツサーバ, 42 値付け部, 43 ポリシー記憶部, 44 セキュ
 アコンテナ作成部, 45 相互認証部, 51 レシーバ, 52 HDD,
 61 通信部, 62 SAM, 63 外部記憶部, 64 伸張部, 65
 通信部, 66 インタフェース, 67 表示制御部, 68 入力制御部,
 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジ
 ュール, 74 復号/暗号化モジュール, 75 データ検査モジュール,
 91 復号ユニット, 92 乱数発生ユニット, 93 暗号化ユニット,
 101 相互認証モジュール, 102 復号モジュール, 103 復号モジ
 ュール, 104 伸張モジュール, 105 ウォータマーク付加モジュール
 , 201 レシーバ, 202 HDD, 211 通信部, 212 SAM,
 213 外部記憶部, 214 伸張部, 215 通信部, 216 インタ
 フェース, 217 表示制御部, 218 入力制御部, 221 相互認証
 モジュール, 222 課金処理モジュール, 223 記憶モジュール, 2
 24 復号/暗号化モジュール, 225 データ検査モジュール, 231
 復号ユニット, 232 乱数発生ユニット, 233 暗号化ユニット, 2
 41 相互認証モジュール, 242 復号モジュール, 243 復号モジ
 ュール, 244 伸張モジュール, 245 ウォータマーク付加モジュール

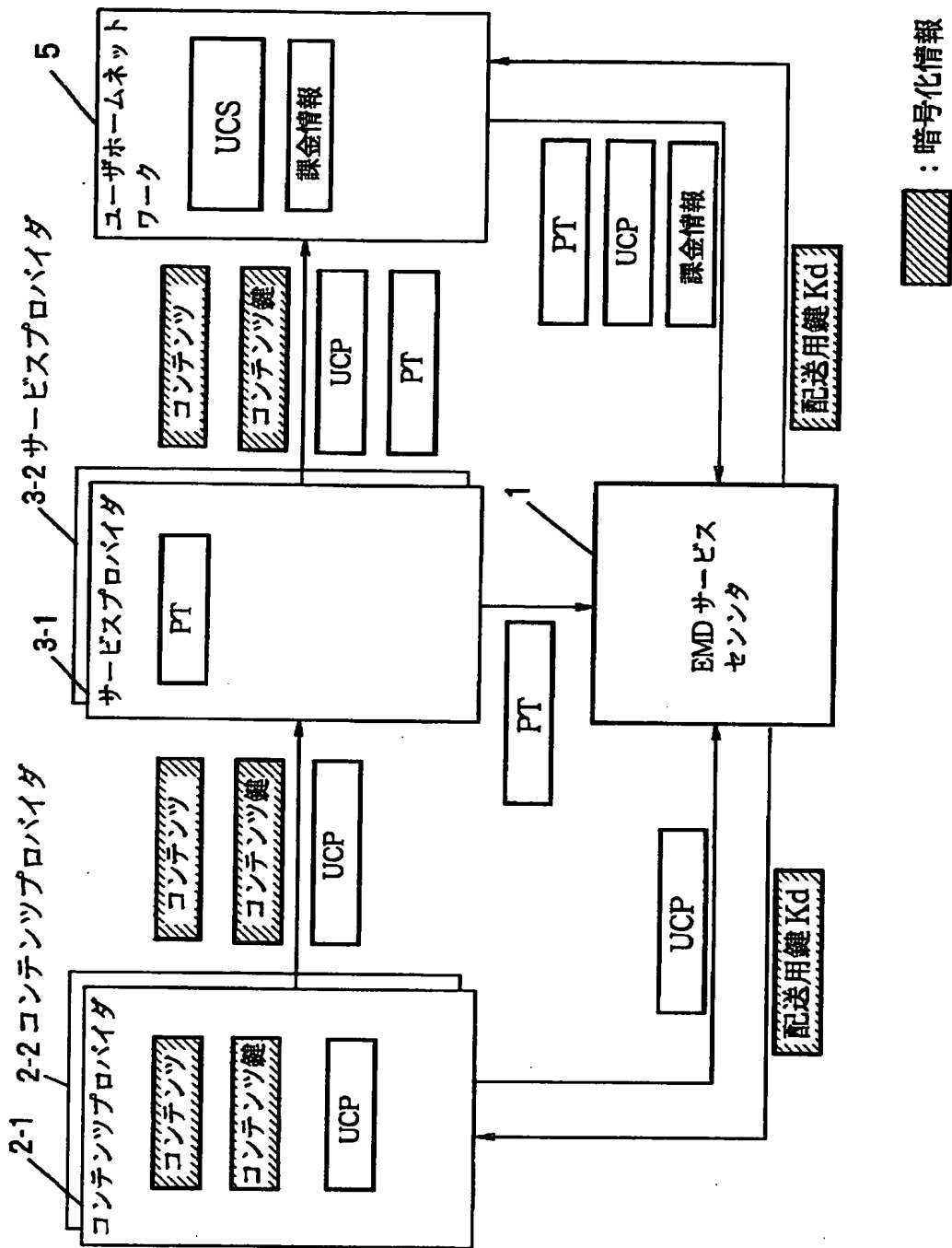
【書類名】

図面

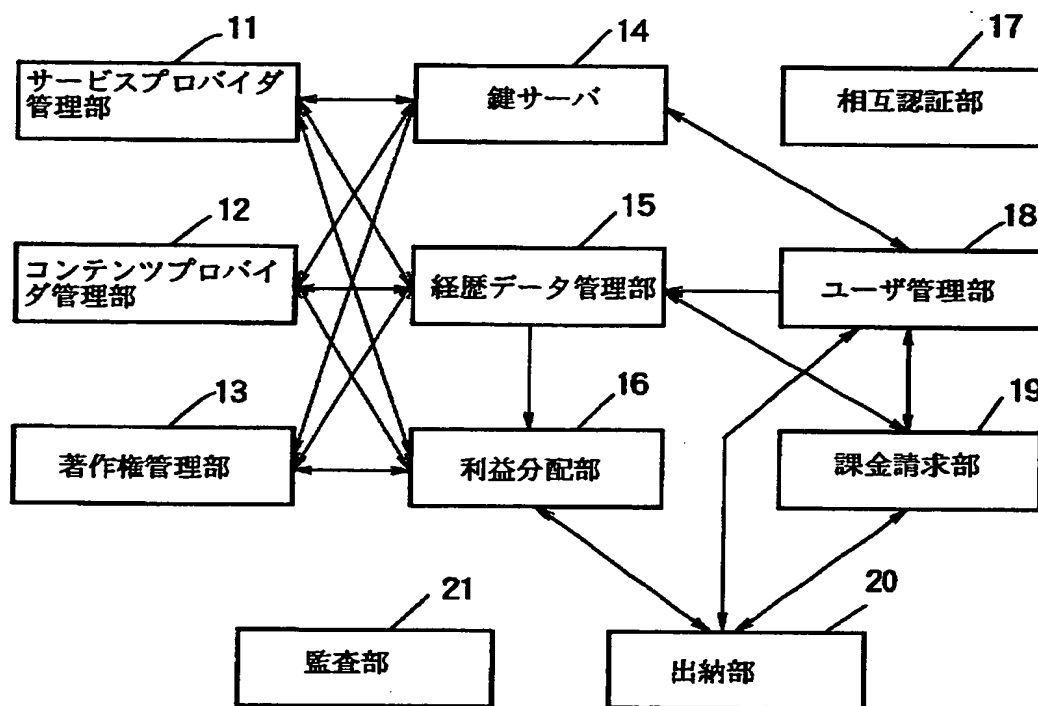
【図 1】



【図 2】

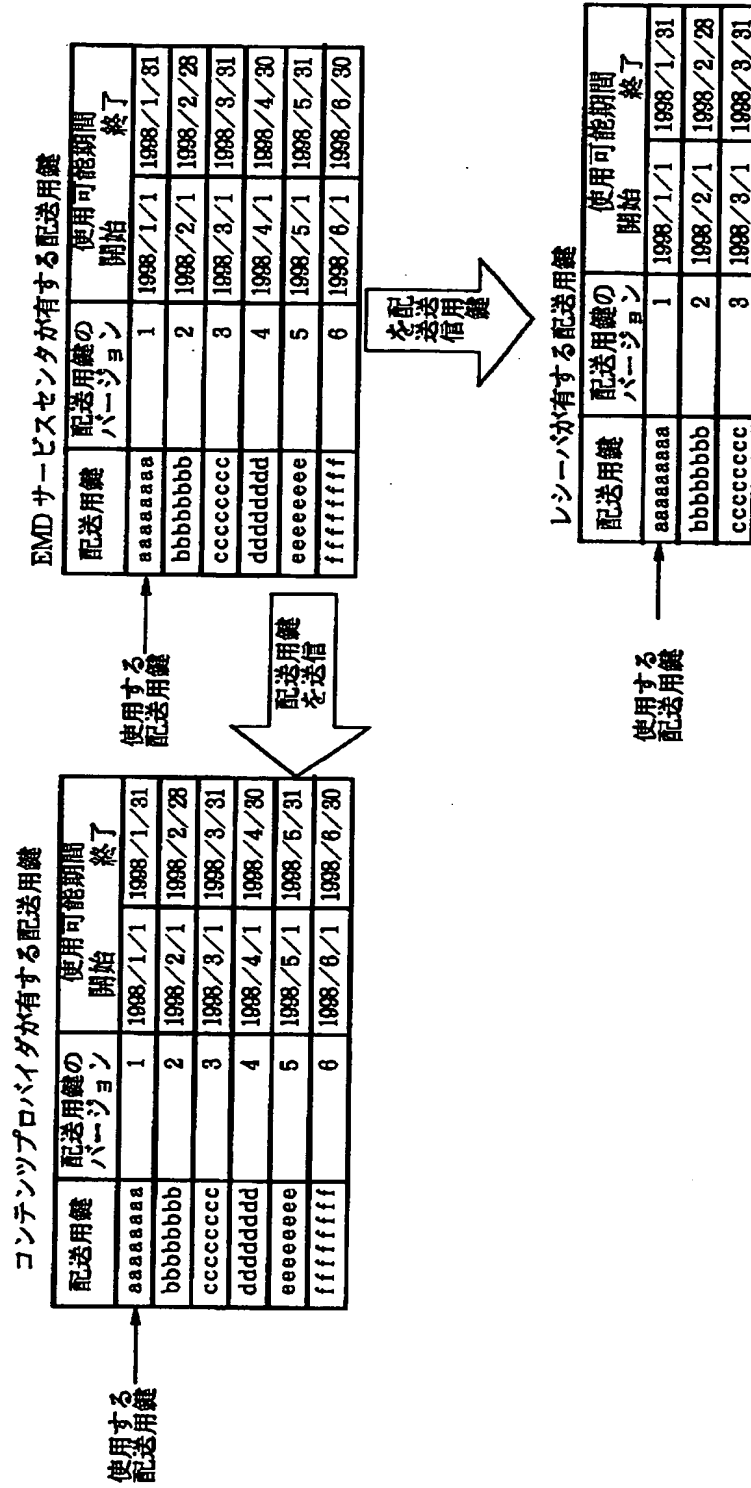


【図 3】

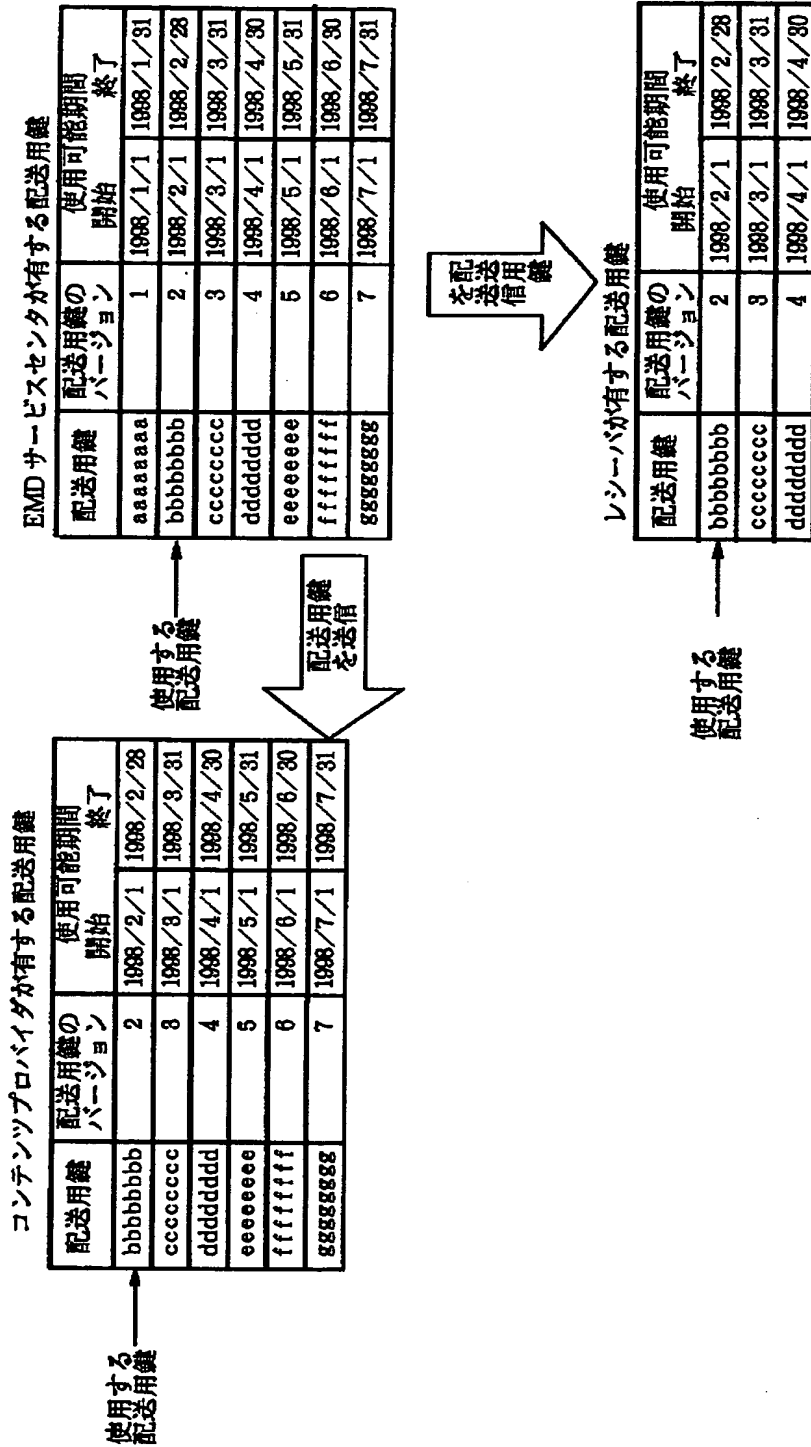


EMD サービスセンタ 1

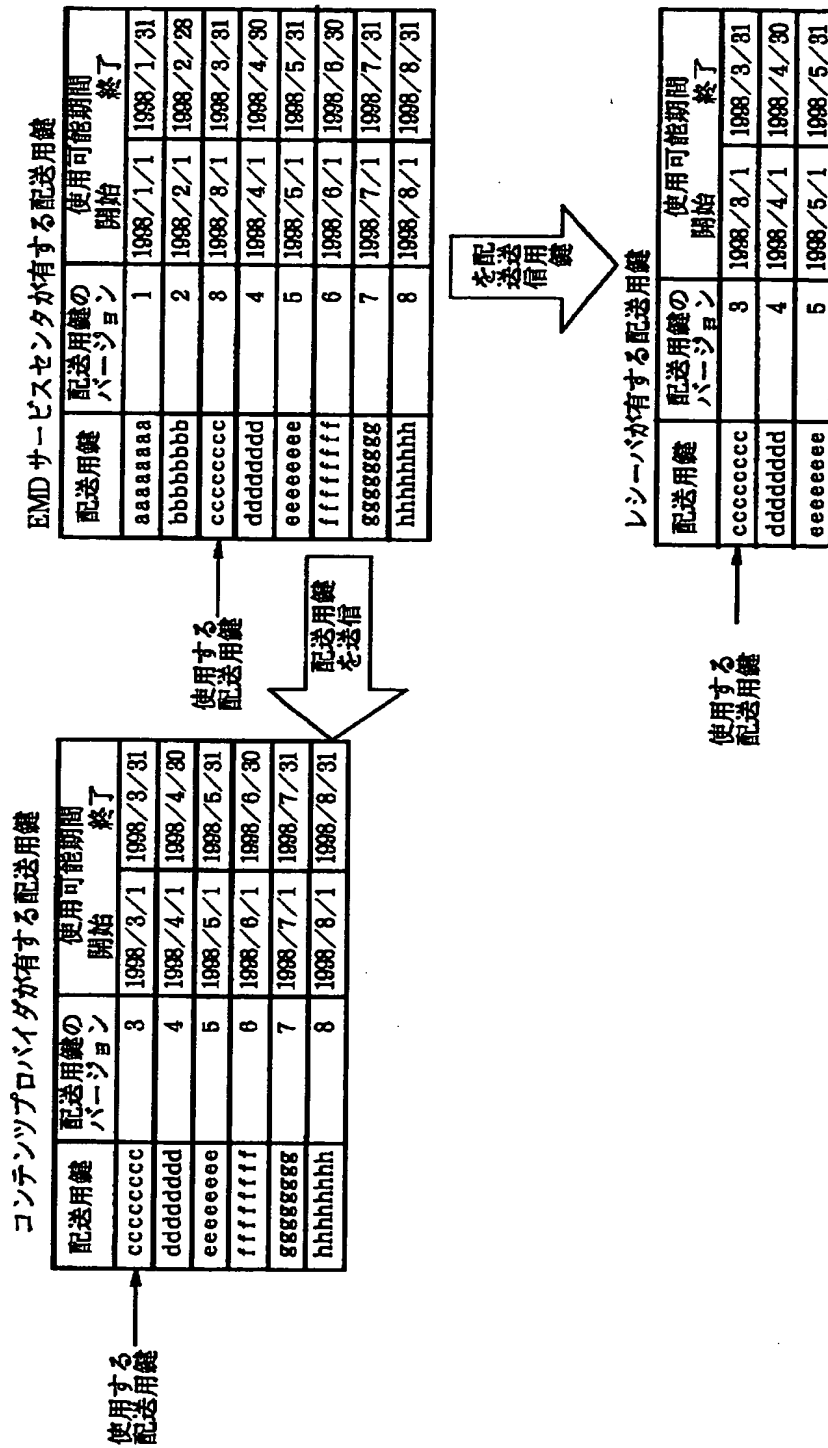
【図 4】



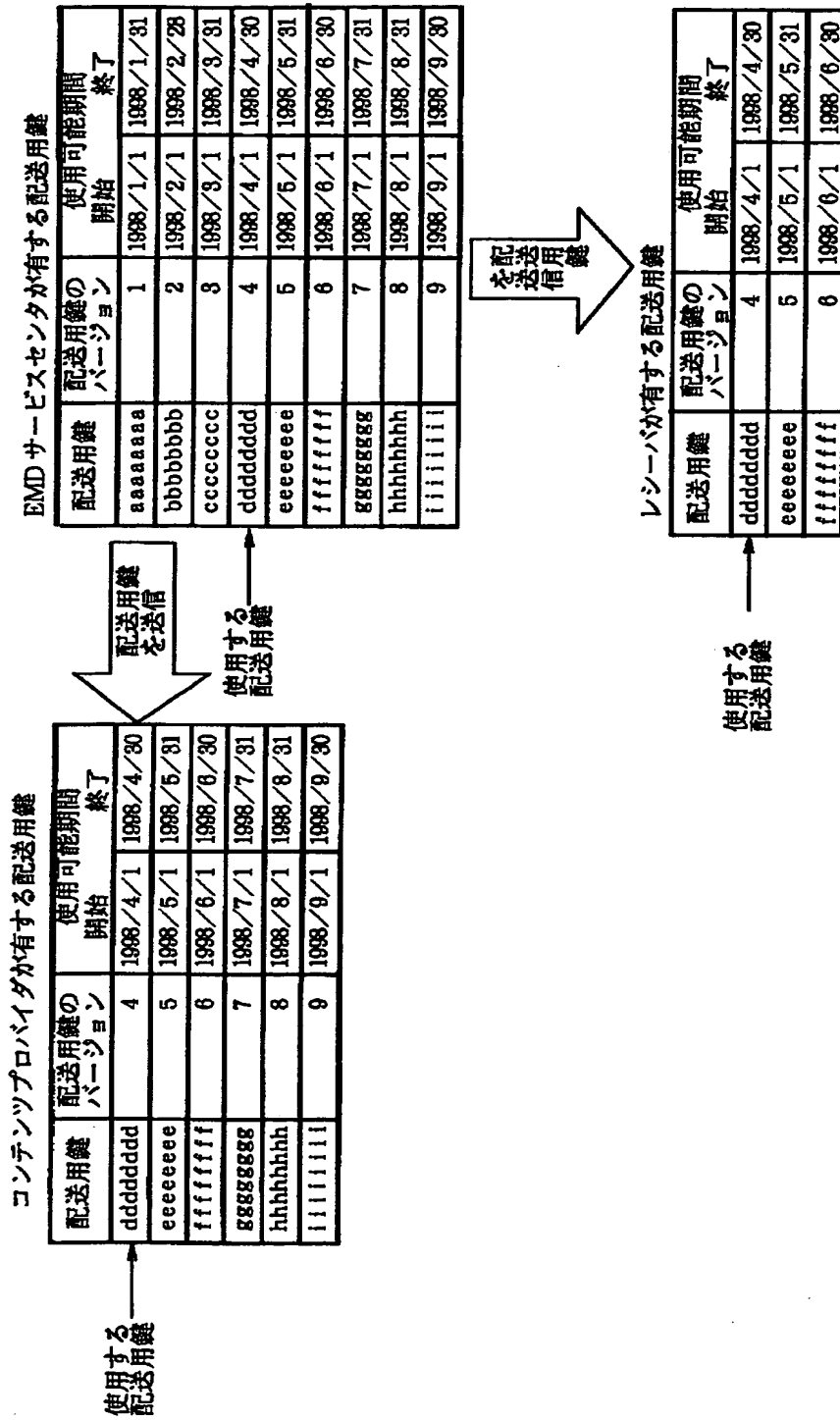
【図 5】



【図 6】



【図 7】



【図 8】

配送用鍵	配送用鍵の バージョン	使用可能期間 開始 終了
aaaaaaaaa	1	1998/1/1 1998/1/31

仮配送用鍵 Kd

【図 9】

SAM の ID		SAM62 の ID	SAM212 の ID
機器番号		レシーバ 51 の 機器番号(100 番)	レシーバ 201 の 機器番号(100 番)
決済 ID		ユーザ F の決済 ID	ユーザ A の決済 ID
決済ユーザ情報	氏名	ユーザ F の氏名	ユーザ A の氏名
	住所	ユーザ F の住所	ユーザ A の住所
	電話番号	ユーザ F の電話番号	ユーザ A の電話番号
	決済機関情報	ユーザ F の決済情報	ユーザ A の決済情報
	生年月日	ユーザ F の生年月日	ユーザ A の生年月日
	年齢	ユーザ F の年齢	ユーザ A の年齢
	性別	ユーザ F の性別(男)	ユーザ A の性別(女)
	ユーザの ID	ユーザ F の ID	ユーザ A の ID
	パスワード	ユーザ F のパスワード	ユーザ A のパスワード
従属ユーザ情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザの ID		
	パスワード		
利用ポイント情報		レシーバ 51 の利用 ポイント情報	レシーバ 201 利用 ポイント情報

システム登録情報

【図 10】

(A)

ユーザ	プロバイダ	利用ポイント
決済 ユーザ	コンテンツプロバイダ 2-1	222 ポイント
	コンテンツプロバイダ 2-2	123 ポイント
	サービスプロバイダ 3-1	345 ポイント
	サービスプロバイダ 3-2	0 ポイント

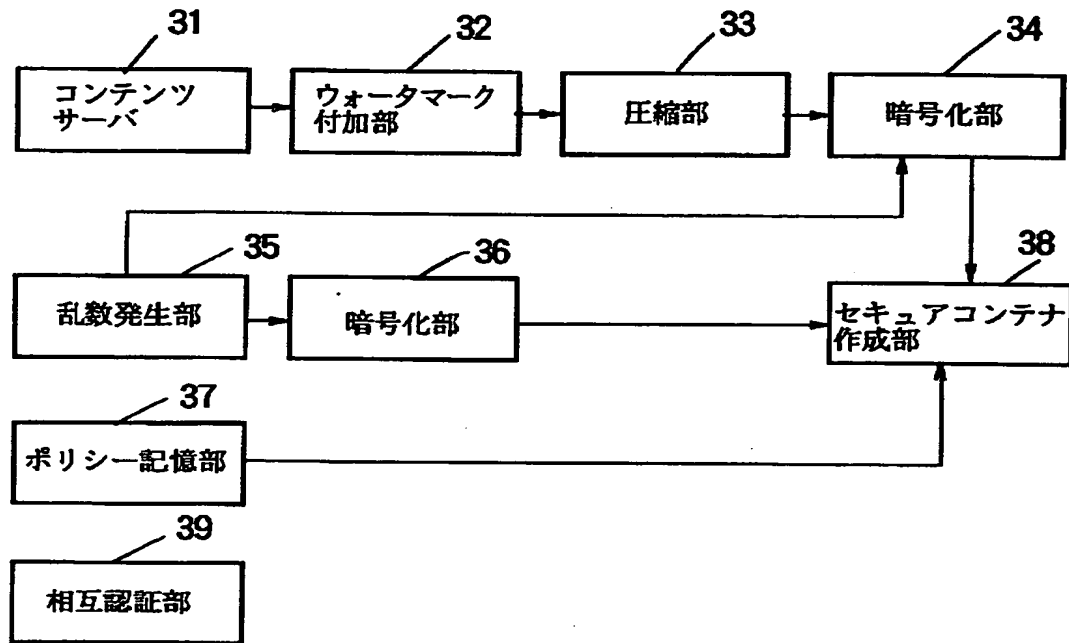
利用ポイント情報

(B)

ユーザ	プロバイダ	利用ポイント
決済 ユーザ	コンテンツプロバイダ 2-1	23 ポイント
	コンテンツプロバイダ 2-2	22 ポイント
	サービスプロバイダ 3-1	40 ポイント
	サービスプロバイダ 3-2	5 ポイント

利用ポイント情報

【図 1 1】



コンテンツプロバイダ 2-1

【図 1 2】

(B)

コンテンツの ID	コンテンツ A の ID
コンテンツプロバイダの ID	コンテンツプロバイダ 2-1 の ID
UCP の ID	ucpB の ID
UCP の有効期限	ucpB の有効期限
利用条件 20	ユーザ条件 20
	機器条件 20
利用内容 21	ID 21
	形式 21
	パラメータ 21
	管理移動許可情報 21
利用内容 22	ID 22
	形式 22
	パラメータ 22
	管理移動許可情報 22

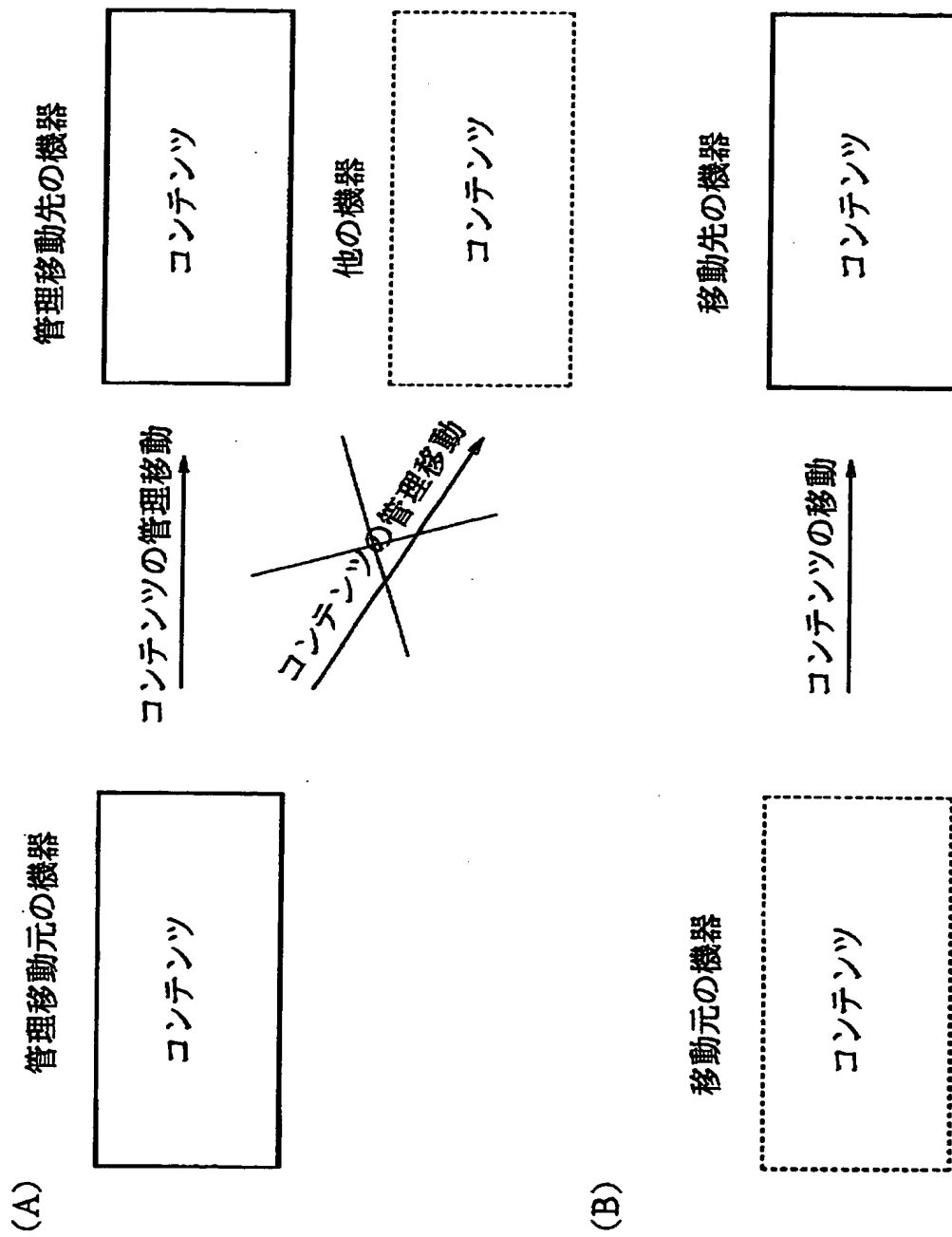
ucpB

(A)

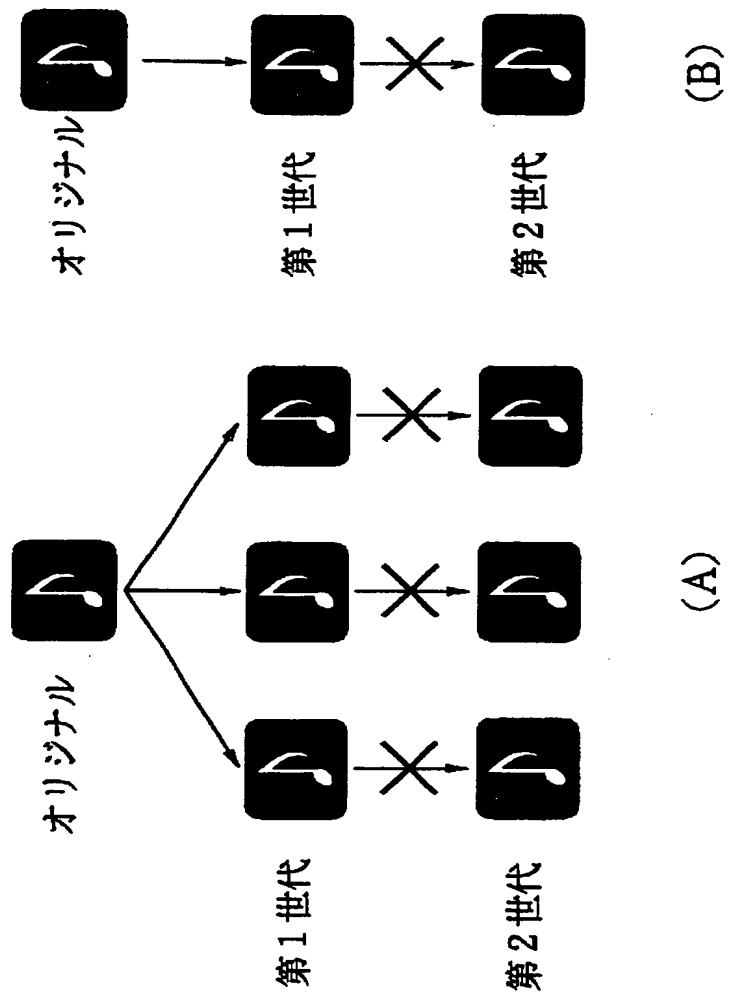
コンテンツの ID	コンテンツ A の ID
コンテンツプロバイダの ID	コンテンツプロバイダ 2-1 の ID
UCP の ID	ucpA の ID
UCP の有効期限	ucpA の有効期限
利用条件 10	ユーザ条件 10
	機器条件 10
利用内容 11	ID 11
	形式 11
	パラメータ 11
	管理移動許可情報 11
利用内容 12	ID 12
	形式 12
	パラメータ 12
	管理移動許可情報 12
利用内容 13	ID 13
	形式 13
	パラメータ 13
	管理移動許可情報 13
利用内容 14	ID 14
	形式 14
	パラメータ 14
	管理移動許可情報 14

ucpA

【図 1 3】



【図 14】



【図 15】

(A)

サービスコード	意 味
0000h	条件なし
0001h 乃至 00FFh	機器に関し条件有り
0100h 乃至 01FFh	性別条件あり
0200h 乃至 02FFh	年令条件あり
0300h 乃至 7FFFh	その他の条件あり
8000h 乃至 FFFFh	利用ポイントに関し条件有り

(B)

コンディションコード	意 味
00h	無条件
01h	=
02h	≠
03h	<(より小さい)
04h	>(より大きい)
05h	≤(以下)
06h	≥(以上)
07h 乃至 FFh	空き

【図16】

(A)

ユーザ条件 10	サービスコード	バリュースコード	コンディションコード
	80××h	0000C8h	06h
機器条件 10	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

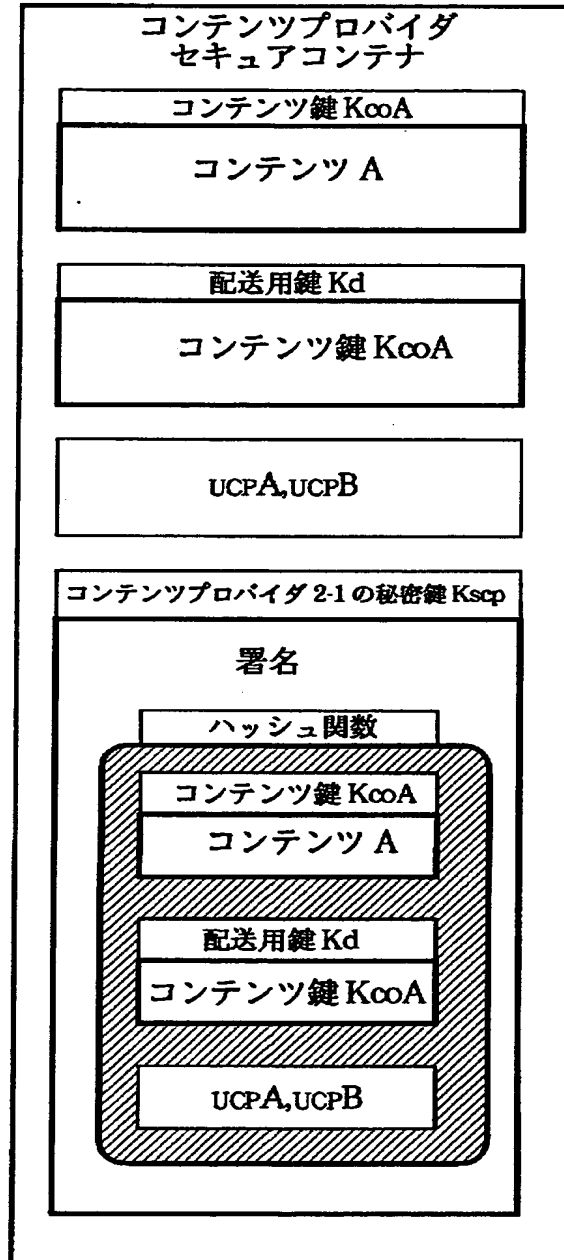
UCPA の利用条件 10

(B)

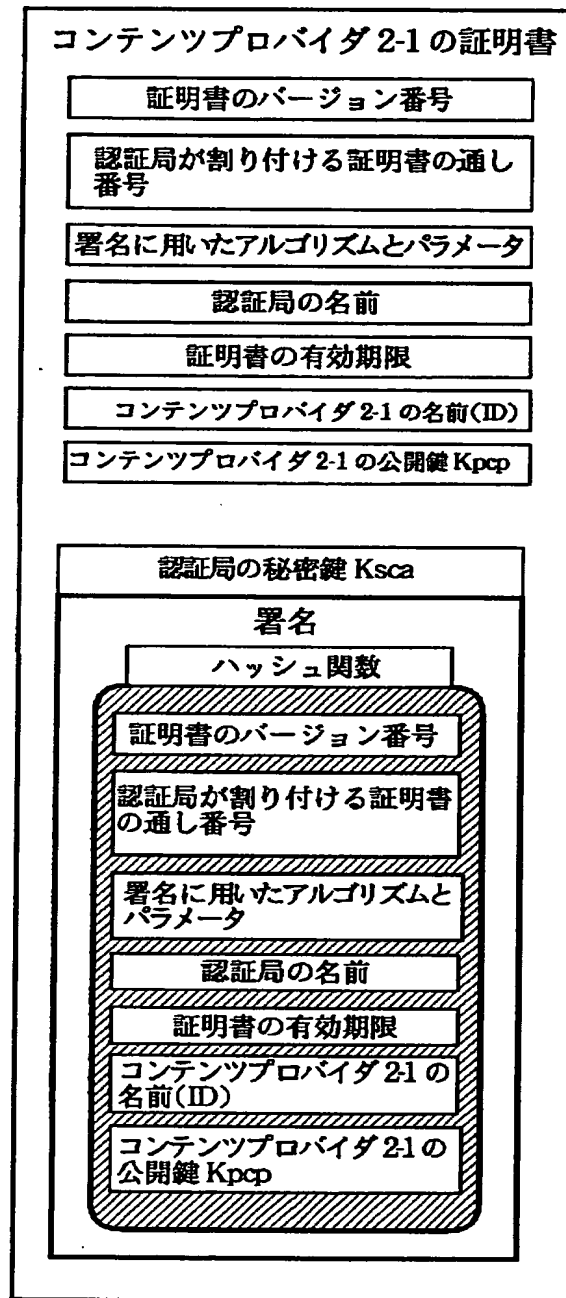
ユーザ条件 20	サービスコード	バリュースコード	コンディションコード
	80××h	0000C8h	03h
機器条件 20	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

UCPB の利用条件 20

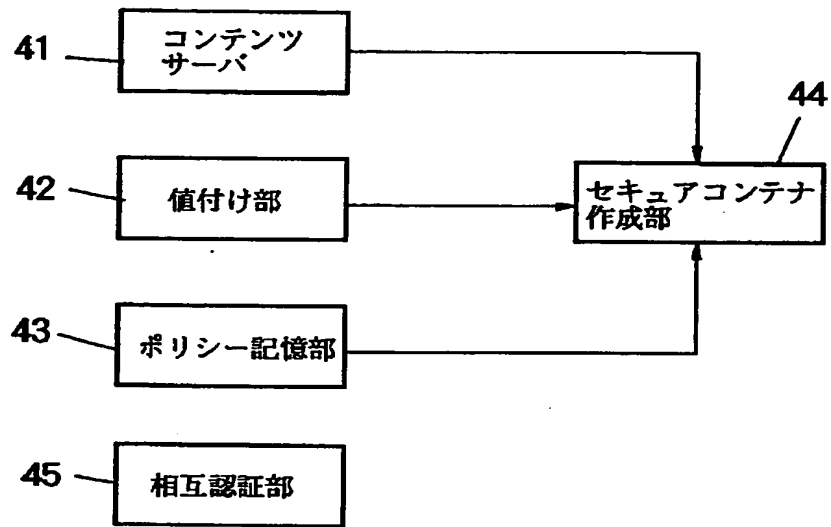
【図 17】



【図 18】



【図 1 9】



サービスプロバイダ 3-1

【図 20】

(B)

コンテンツの ID	コンテンツ A の ID	
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID	
UCP の ID	ucpA の ID	
サービス プロバイダの ID	サービスプロバイダ 3-1 の ID	
PT の ID	ptA-2 の ID	
PT の有効期限	ptA-2 の有効期限	
価格条件 20	ユーザ条件 20	女性
	機器条件 20	条件なし
価格内容 21	1000 円	
価格内容 22	300 円	
価格内容 23	50 円	
価格内容 24	150 円	

PTA-2

(A)

コンテンツの ID	コンテンツ A の ID	
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID	
UCP の ID	ucpA の ID	
サービス プロバイダの ID	サービスプロバイダ 3-1 の ID	
PT の ID	PTA-1 の ID	
PT の有効期限	PTA-1 の有効期限	
価格条件 10	ユーザ条件 10	男性
	機器条件 10	条件なし
価格内容 11	2000 円	
価格内容 12	600 円	
価格内容 13	100 円	
価格内容 14	300 円	

PTA-1

【図 2 1】

(A)

ユーザ 条件 10	サービスコード	バリュースコード	コンディションコード
	01 × × h	000000h	01h
機器条件 10	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1 の価格条件 10

(B)

ユーザ 条件 20	サービスコード	バリュースコード	コンディションコード
	01 × × h	000001h	01h
機器 条件 20	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2 の価格条件 20

【図 22】

コンテンツの ID	コンテンツ A の ID		
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID		
UCP の ID	ucpB の ID		
サービス プロバイダの ID	サービスプロバイダ 8-1 の ID		
PT の ID	PtB-2 の ID		
PT の有効期限	PtB-2 の有効期限		
価格条件 40	ユーザ条件 40	条件なし	
	機器条件 40	主機器	
価格内容 41	50 円		
価格内容 42	150 円		

ptB-2

(B)

コンテンツの ID	コンテンツ A の ID		
コンテンツ プロバイダの ID	コンテンツプロバイダ 2-1 の ID		
UCP の ID	ucpB の ID		
サービス プロバイダの ID	サービスプロバイダ 3-1 の ID		
PT の ID	ptB-1 の ID		
PT の有効期限	ptB-1 の有効期限		
価格条件 30	ユーザ条件 30	条件なし	
	機器条件 30	従機器	
価格内容 31	100 円		
価格内容 32	300 円		

ptB-1

(A)

【図 23】

(A)

ユーザ条件 30	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリューコード	コンディションコード
	00××h	000064h	03h

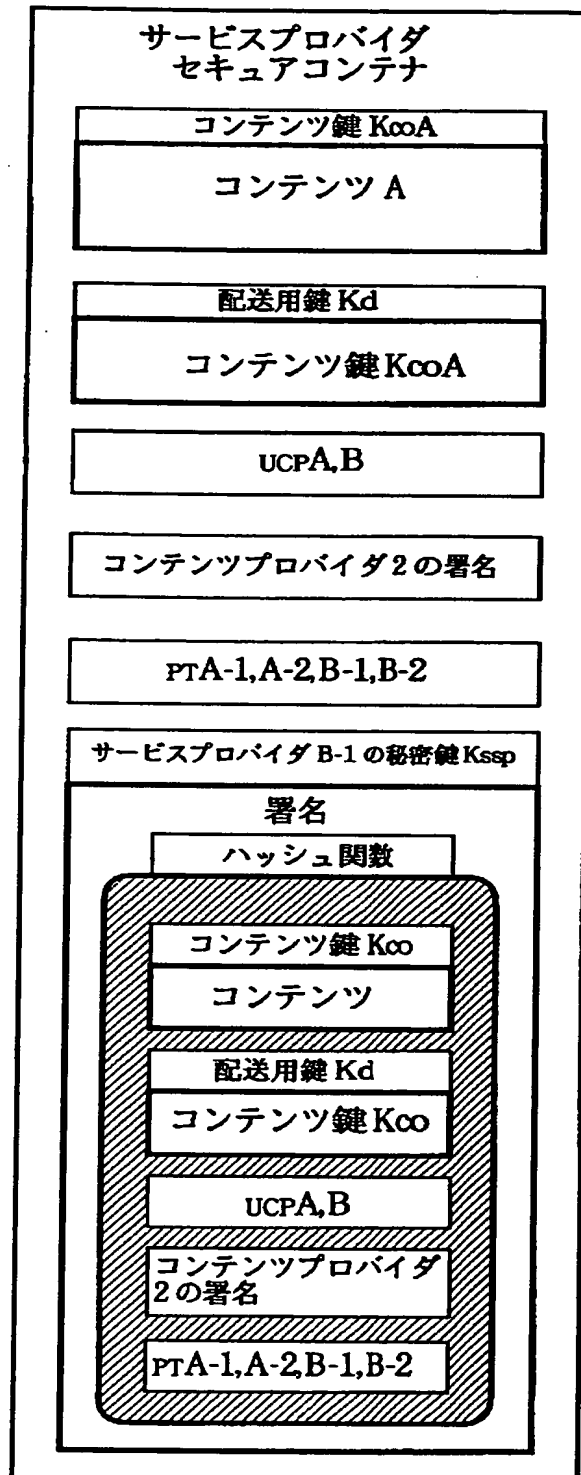
PTB-1 の価格条件 30

(B)

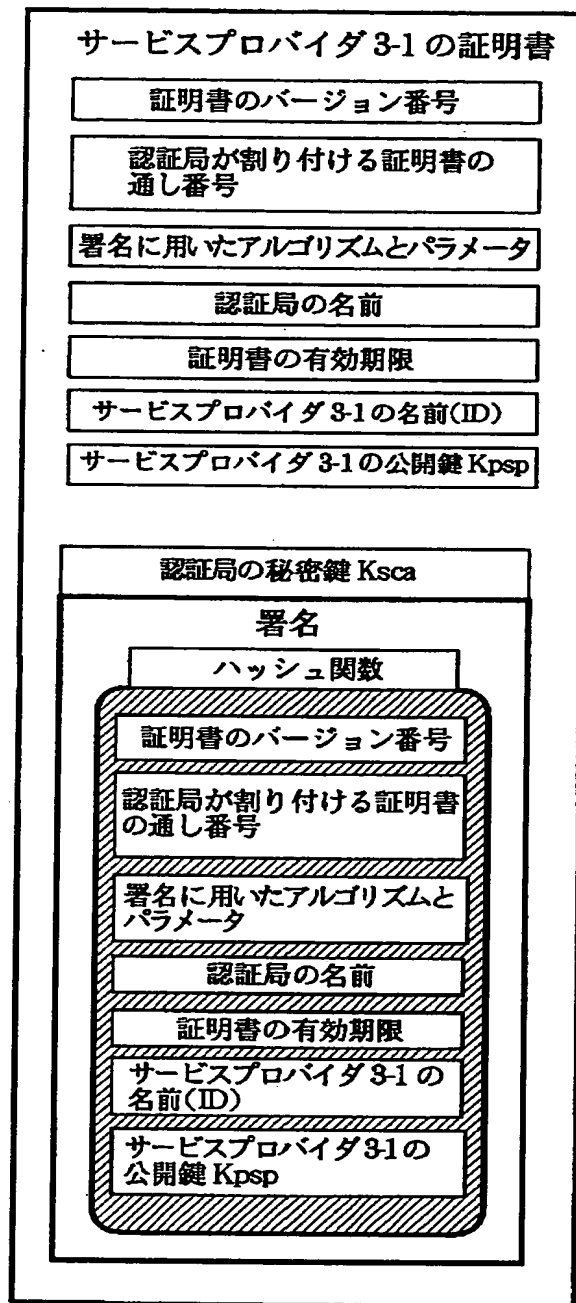
ユーザ条件 40	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリューコード	コンディションコード
	00××h	000064h	06h

PTB-2 の価格条件 40

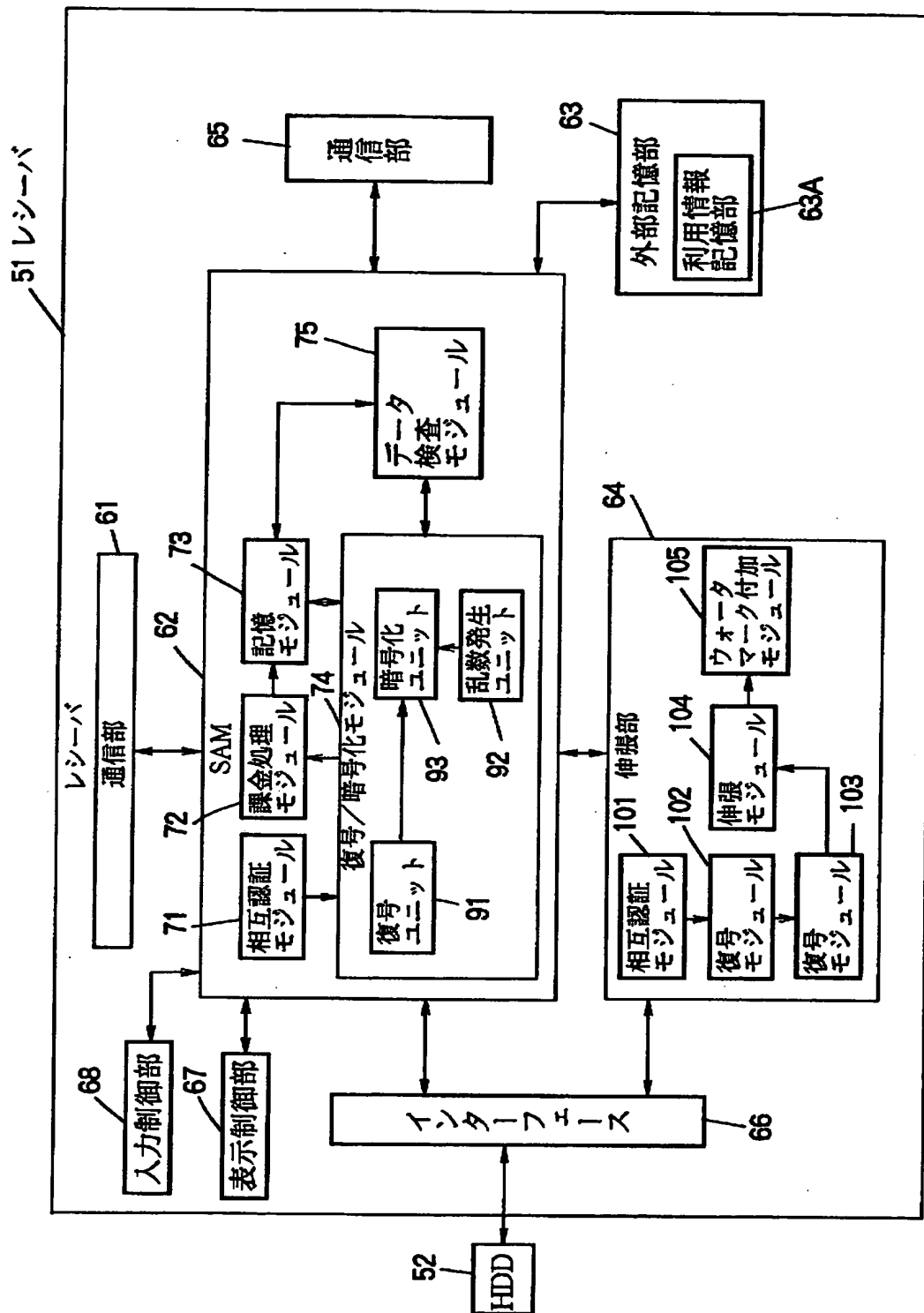
【図 24】



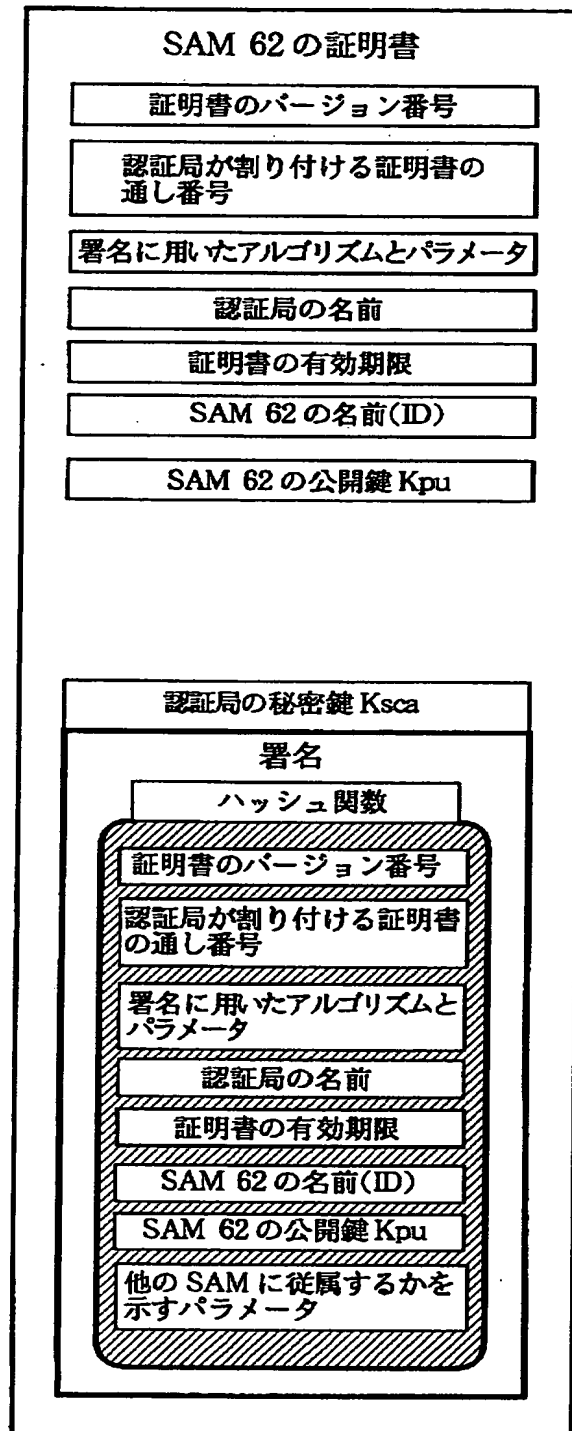
【図 25】



【图 26】



【図 27】

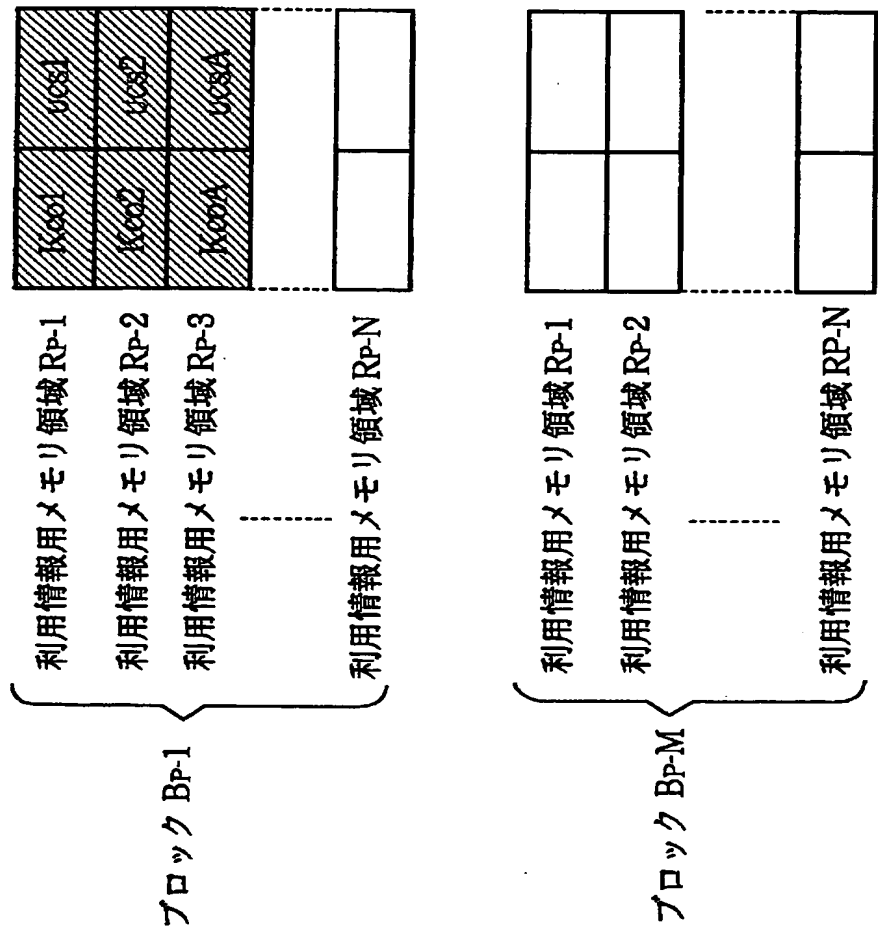


【図 28】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2-1 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3-1 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 11 の ID
	形式	買い取り再生
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID
利用履歴		×××

ucsA

【図 2 9】



利用情報記憶部 63A

【図 30】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2-1 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3-1 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 11 の ID
	形式	買い取り再生
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID
課金履歴		×××

課金情報 A

【図 3 1】

SAM62 の公開鍵 Kpu	
SAM62 の秘密鍵 Ksu	
EMD サービスセンタ 1 の公開鍵 Kpesc	
認証局の公開鍵 Kpca	
保存用鍵 Ksave	
3 月分の配送用鍵 Kd	
⋮	
SAM62 の証明書	
基準情報 51	
課金情報	
⋮	
検査値 Hp-1	検査値 Hp-2 -----
-----	検査値 Hp-M

【図 3 2】

SAM の ID		SAM62 の ID
機器番号		レシーバ 51 の機器番号 (100 番)
決済 ID		ユーザ F の決済 ID
課金の上限額		正式登録時の課金の 上限額
決済 ユーザ 情報	氏名	ユーザ F の氏名
	住所	ユーザ F の住所
	電話番号	ユーザ F の電話番号
	決済機関情報	ユーザ F の決済機関情報
	生年月日	ユーザ F の生年月日
	年齢	ユーザ F の年齢(21 才)
	性別	ユーザ F の性別(男)
	ユーザの ID	ユーザ F の ID
	パスワード	ユーザ F のパスワード
従属 ユーザ 情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザの ID	
	パスワード	
⋮		
利用ポイント情報		レシーバ 51 の利用 ポイント情報

基準情報 51

【図 3 3】

ユーザ	プロバイダ	利用ポイント
決済 ユーザ	コンテンツプロバイダ 2-1	222 ポイント
	コンテンツプロバイダ 2-2	123 ポイント
	サービスプロバイダ 3-1	345 ポイント
	サービスプロバイダ 3-2	0 ポイント

基準情報 51 の利用ポイント情報

【图 3 4】

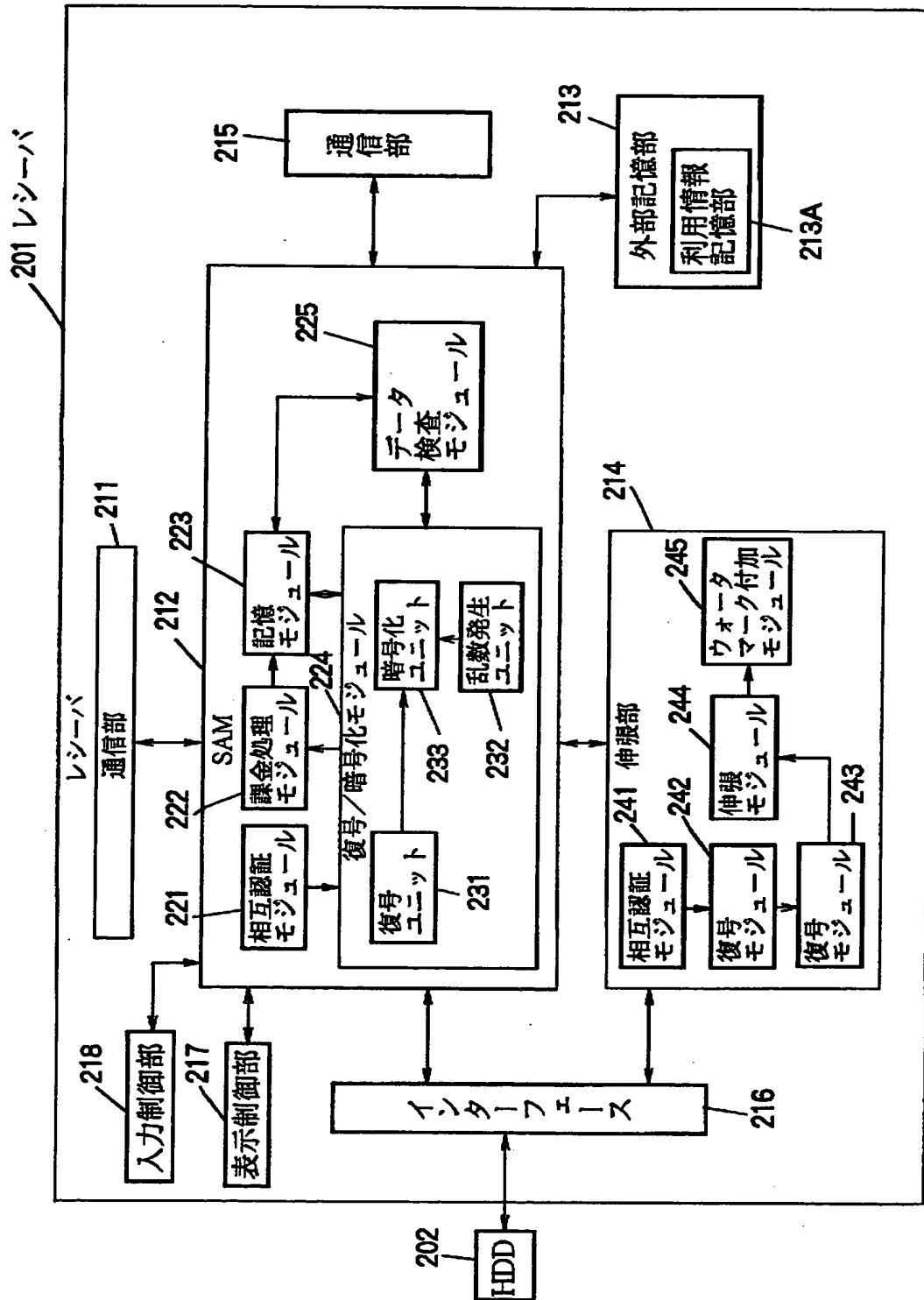
SAM ID	ユーザ ID	購入 処理	課金 処理	課金機器	コンテンツ 供給機器	状態 フラグ	登録条件 署名	登録リス ト署名
SAM62 の ID	ユーザ F の ID	可	可	SAM62 の ID	なし	制限 なし	××××	××××

レシーバ
51の登録
条件

The diagram illustrates the structure of SAM information objects. It consists of two main parts connected by a bracket. The left part is a table with two columns: '対象 SAM ID' (Target SAM ID) and '有効期限' (Expiration Date). The right part is a table with two columns: '対象 SAM 情報部' (Target SAM Information Section) and '接続されている機器数' (Number of connected devices). The '対象 SAM ID' column is linked to the '対象 SAM 情報部' column, and the '有効期限' column is linked to the '接続されている機器数' column.

対象 SAM ID	有効期限	対象 SAM 情報部	接続されている機器数
××××	××××	××××	1

【図 3 5】



【図 3 6】

SAM212 の公開鍵 Kpu	
SAM212 の秘密鍵 Ksu	
EMD サービスセンタ 1 の公開鍵 kpesc	
認証局の公開鍵 Kpca	
保存用鍵 Ksave	
3 月分の配送用鍵 Kd	
⋮	
SAM212 の証明書	
基準情報 201	
⋮	
検査値 Hp-1	検査値 Hp-2
⋮	
検査値 Hp-M	

【図 37】

SAM の ID		SAM62 の ID
機器番号		レシーバ 201 の機器番号 (100 番)
決済 ID		ユーザ A の決済 ID
課金の上限額		正式登録時の上限額
決済 ユーザ 情報	氏名	ユーザ A の氏名
	住所	ユーザ A の住所
	電話番号	ユーザ A の電話番号
	決済機関情報	ユーザ A の決済機関情報
	生年月日	ユーザ A の生年月日
	年齢	ユーザ A の年齢
	性別	ユーザ A の性別
	ユーザの ID	ユーザ A の ID
	パスワード	ユーザ A のパスワード
従属 ユーザ 情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザの ID	
	パスワード	
利用ポイント情報		レシーバ 201 の 利用ポイント情報

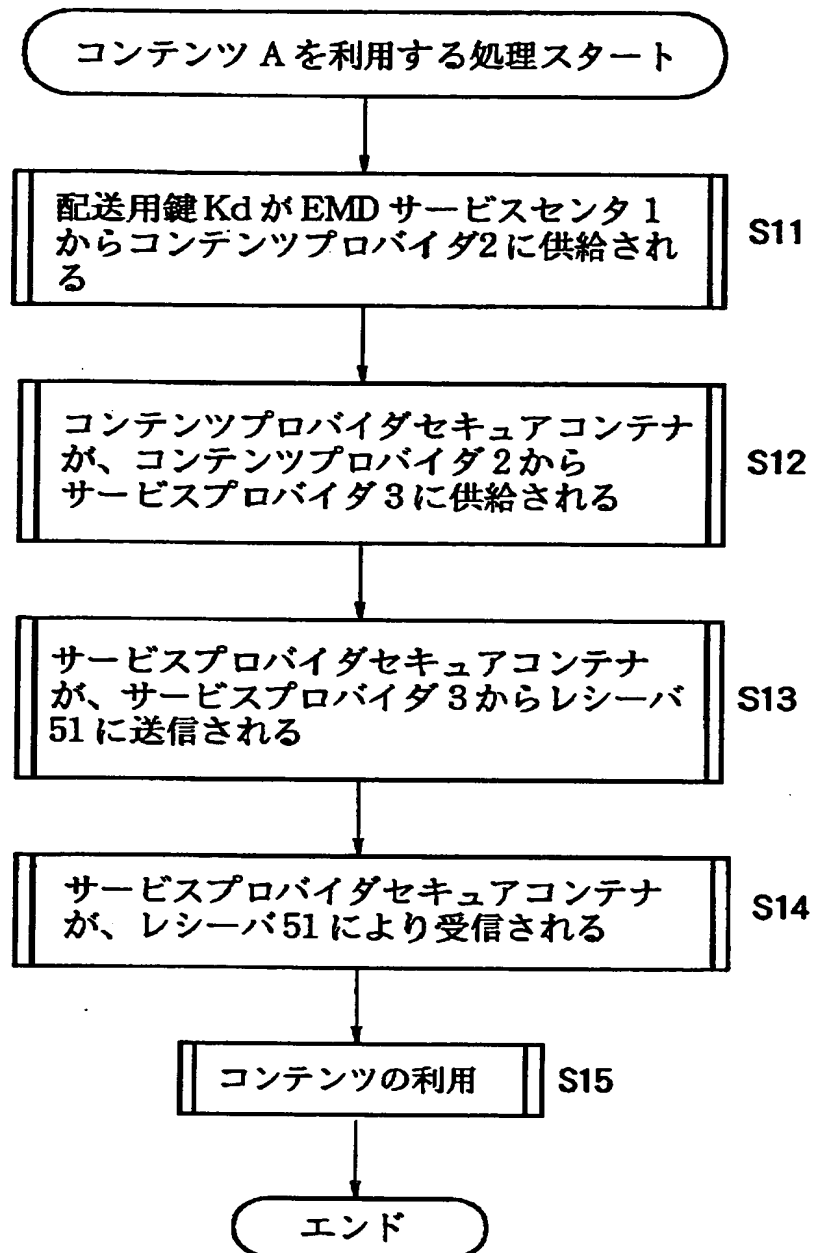
基準情報 201

【図 38】

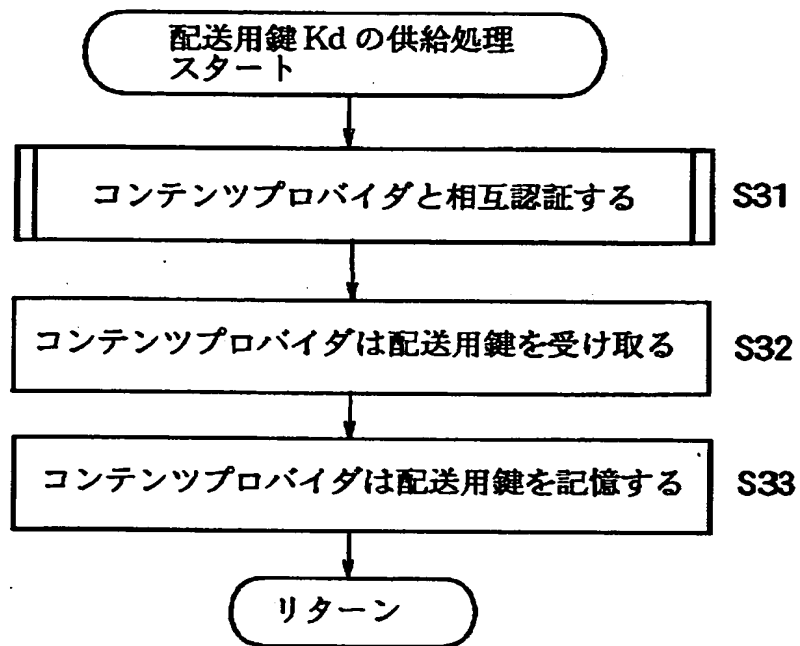
ユーザ	プロバイダ	利用ポイント
決済 ユーザ	コンテンツプロバイダ 2-1	23 ポイント
	コンテンツプロバイダ 2-2	22 ポイント
	サービスプロバイダ 3-1	40 ポイント
	サービスプロバイダ 3-2	5 ポイント

基準情報 201 の利用ポイント情報

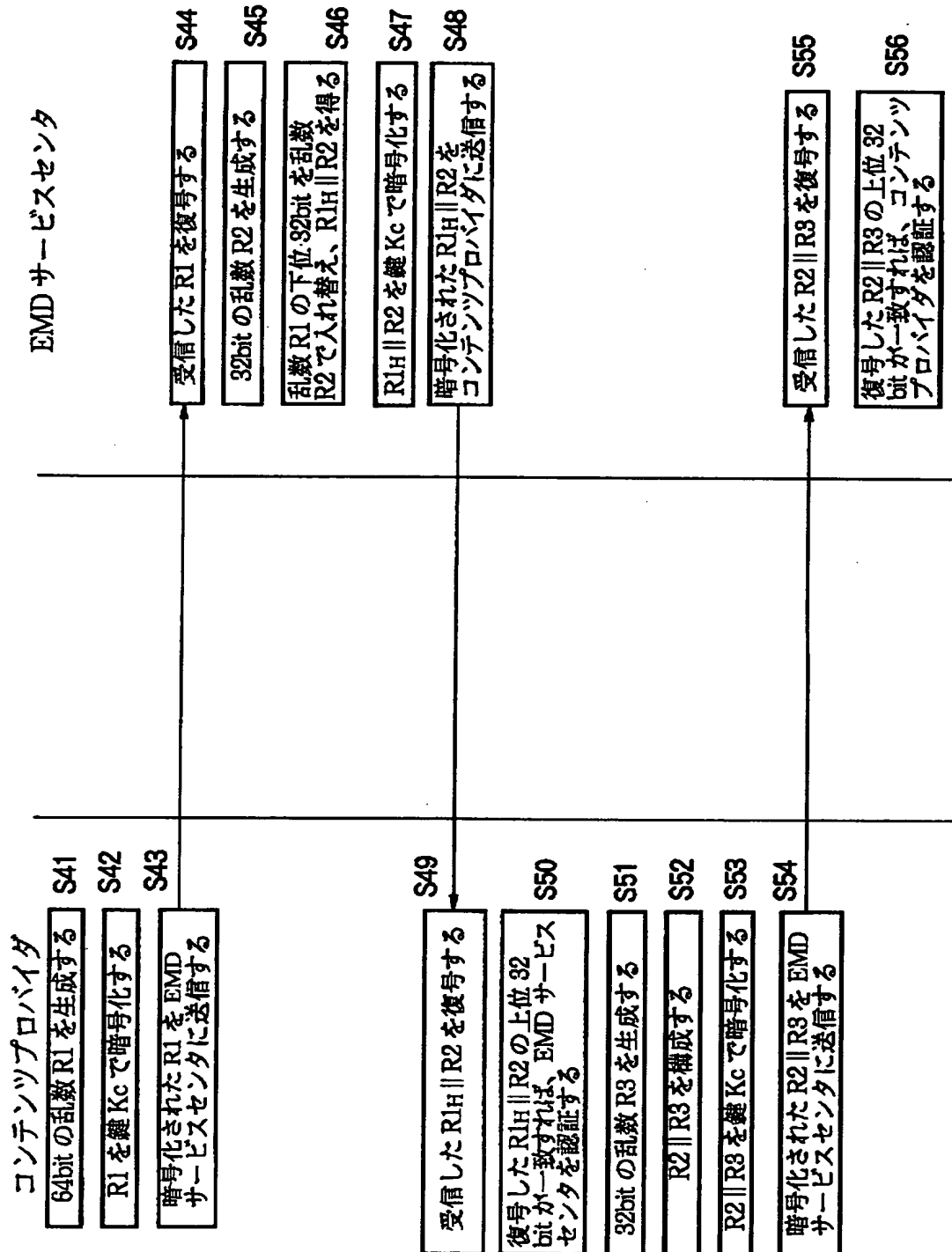
【図 3 9】



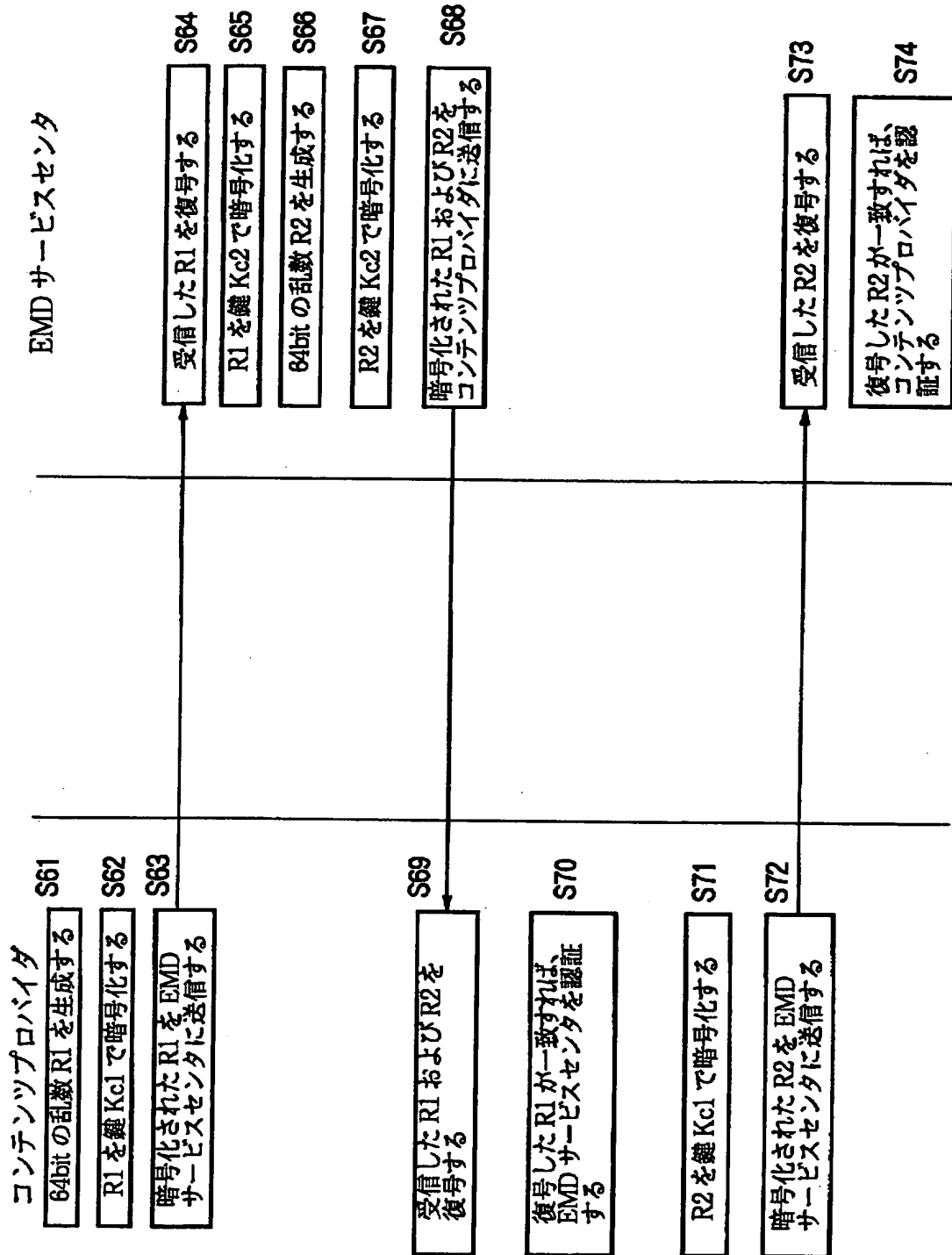
【図 40】



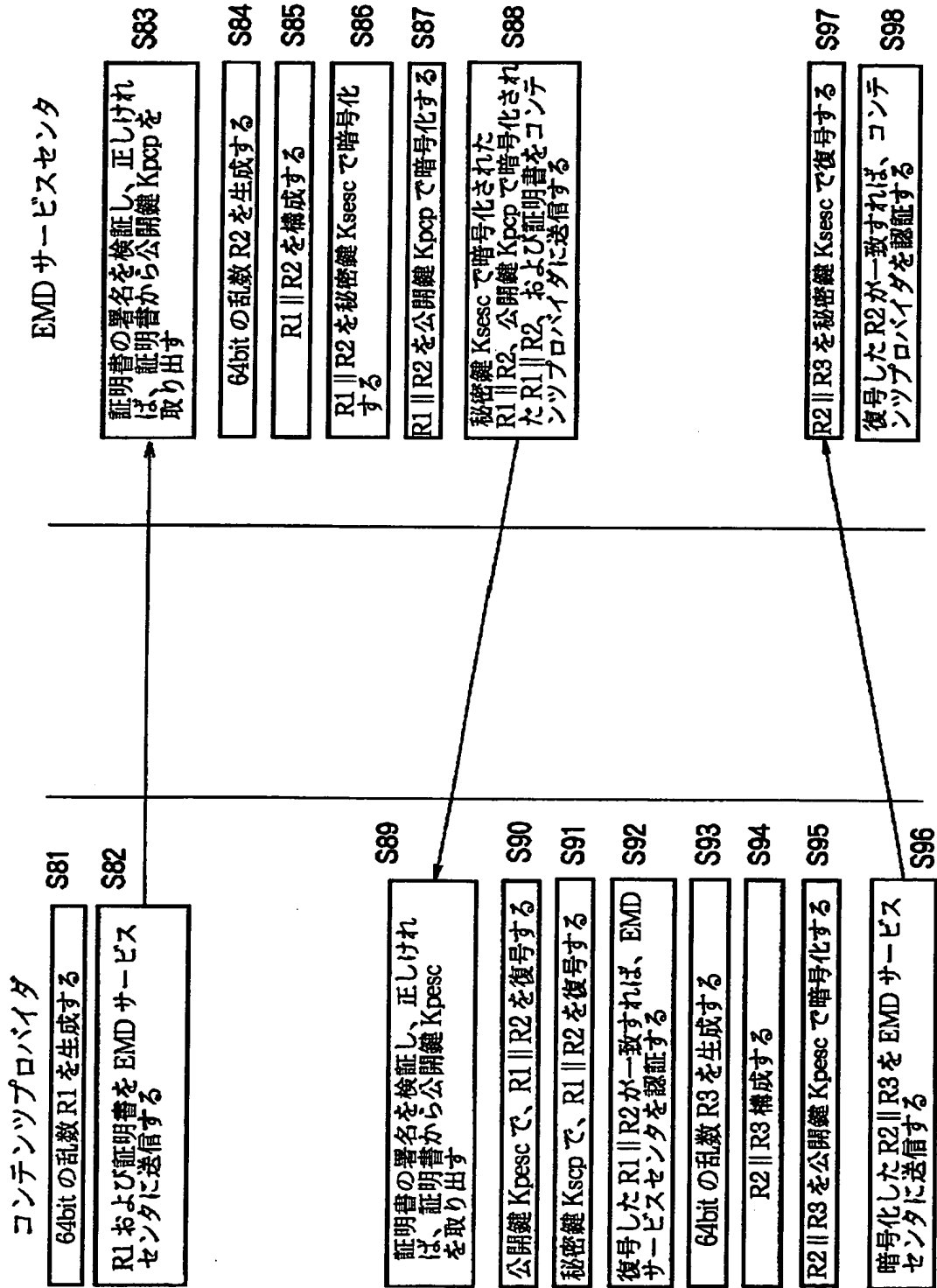
【図 4 1】



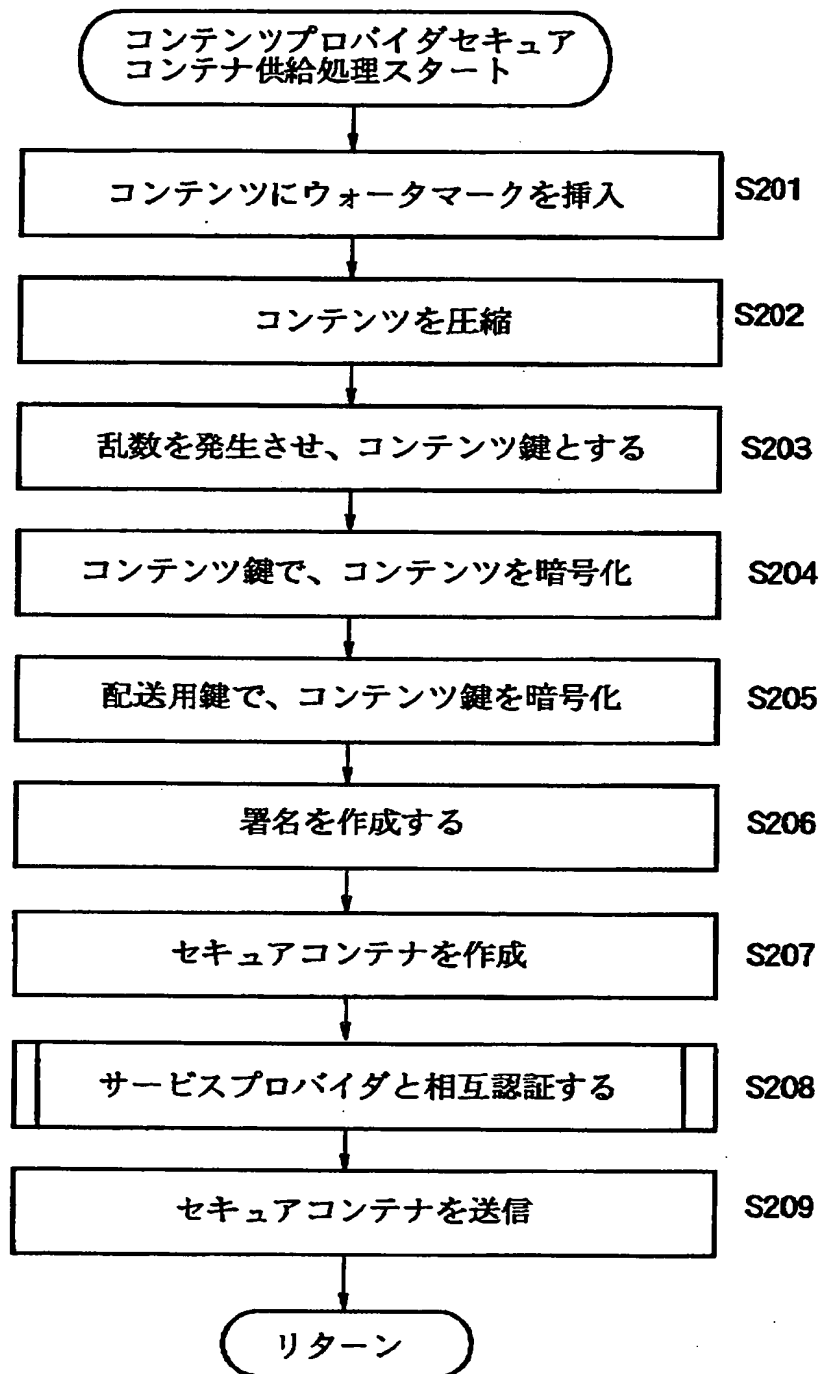
【図 4 2】



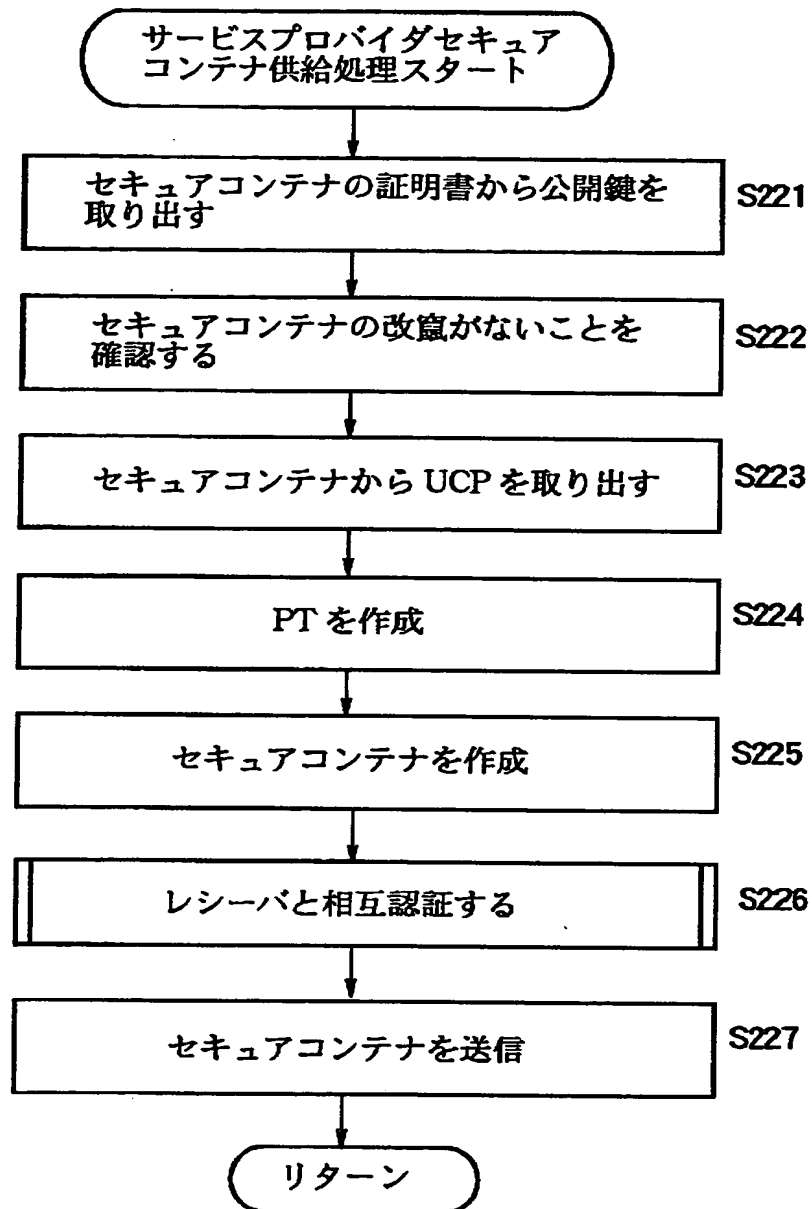
【図 4 3】



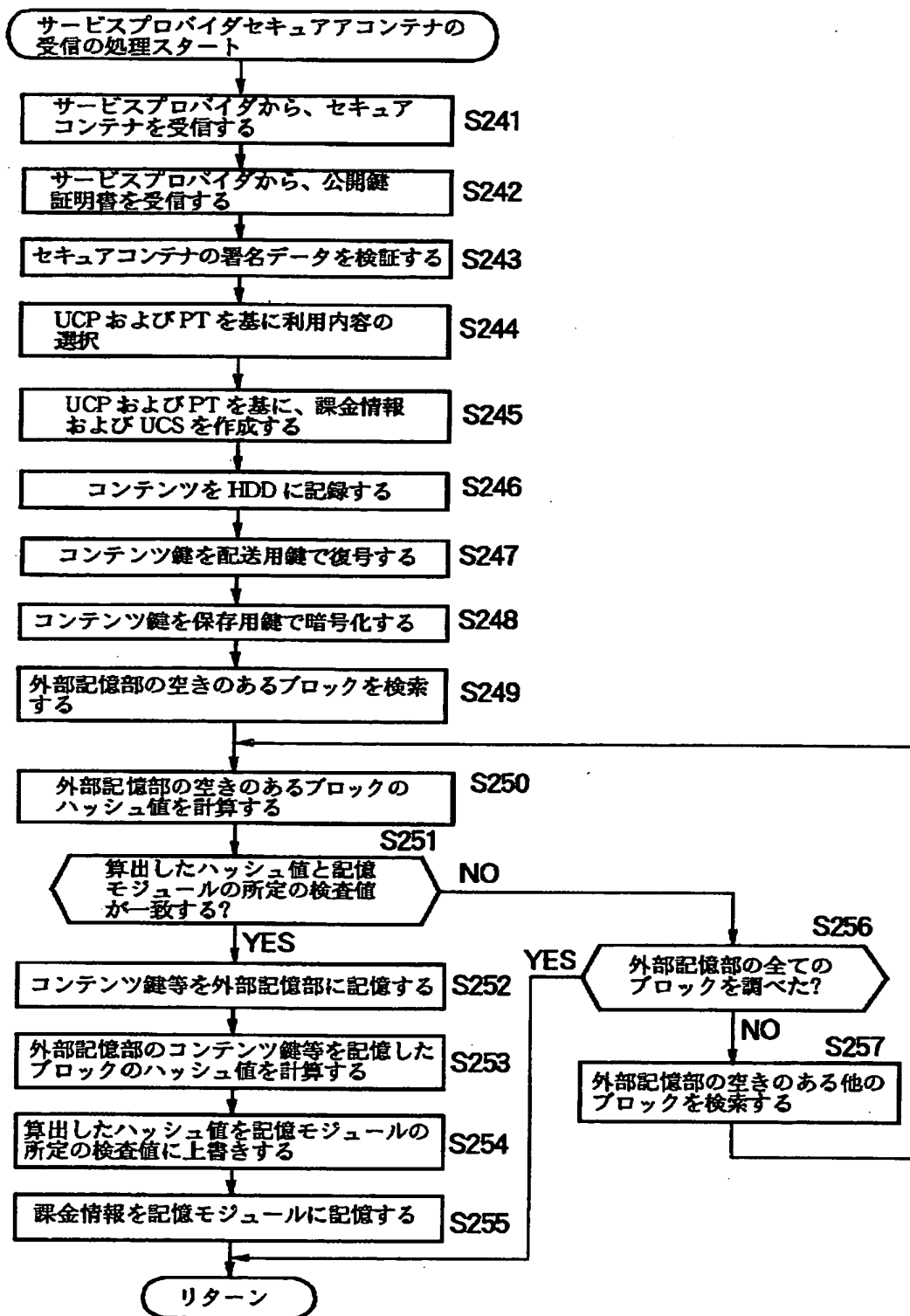
【図 4 4】



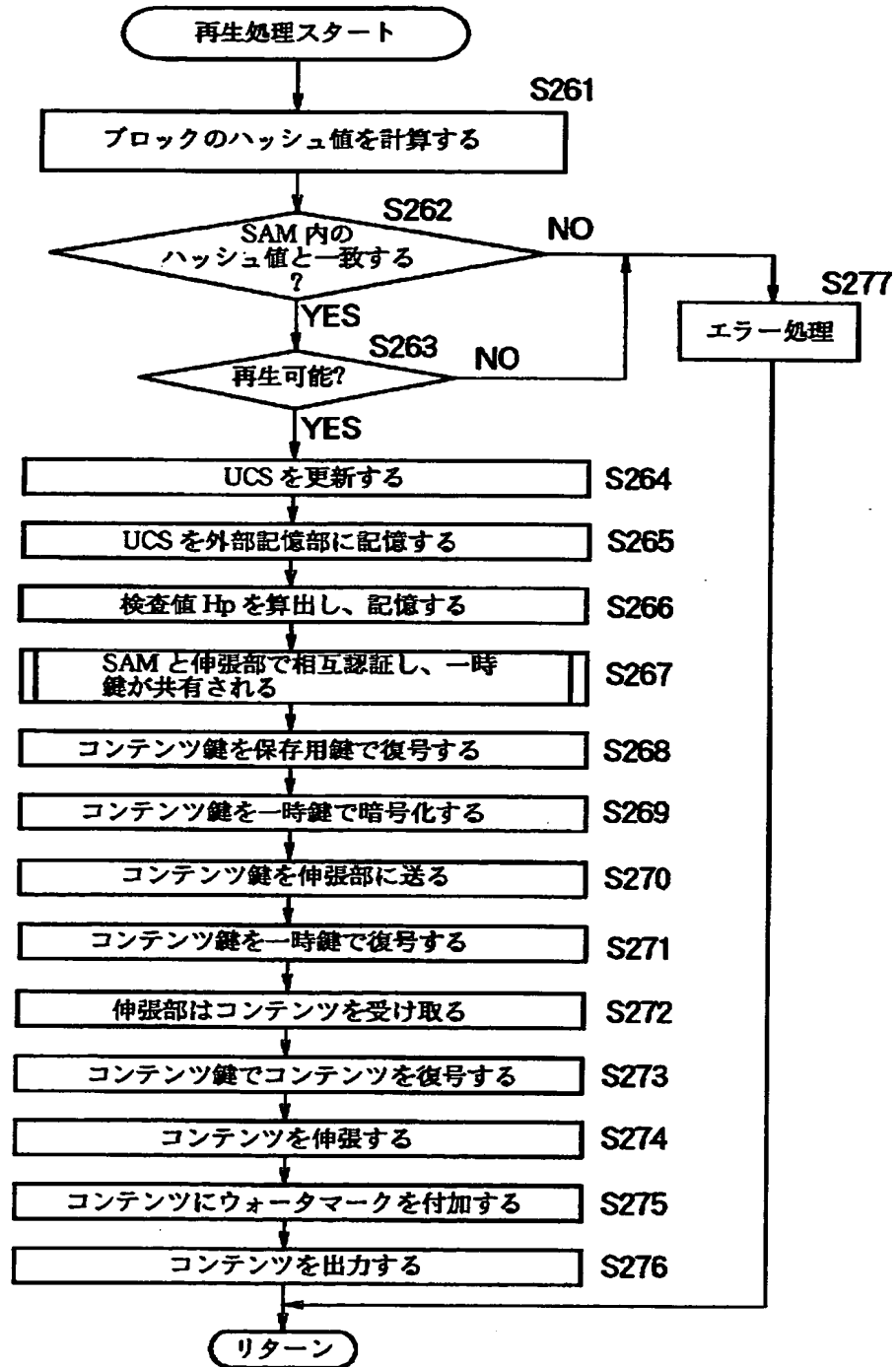
【図 45】



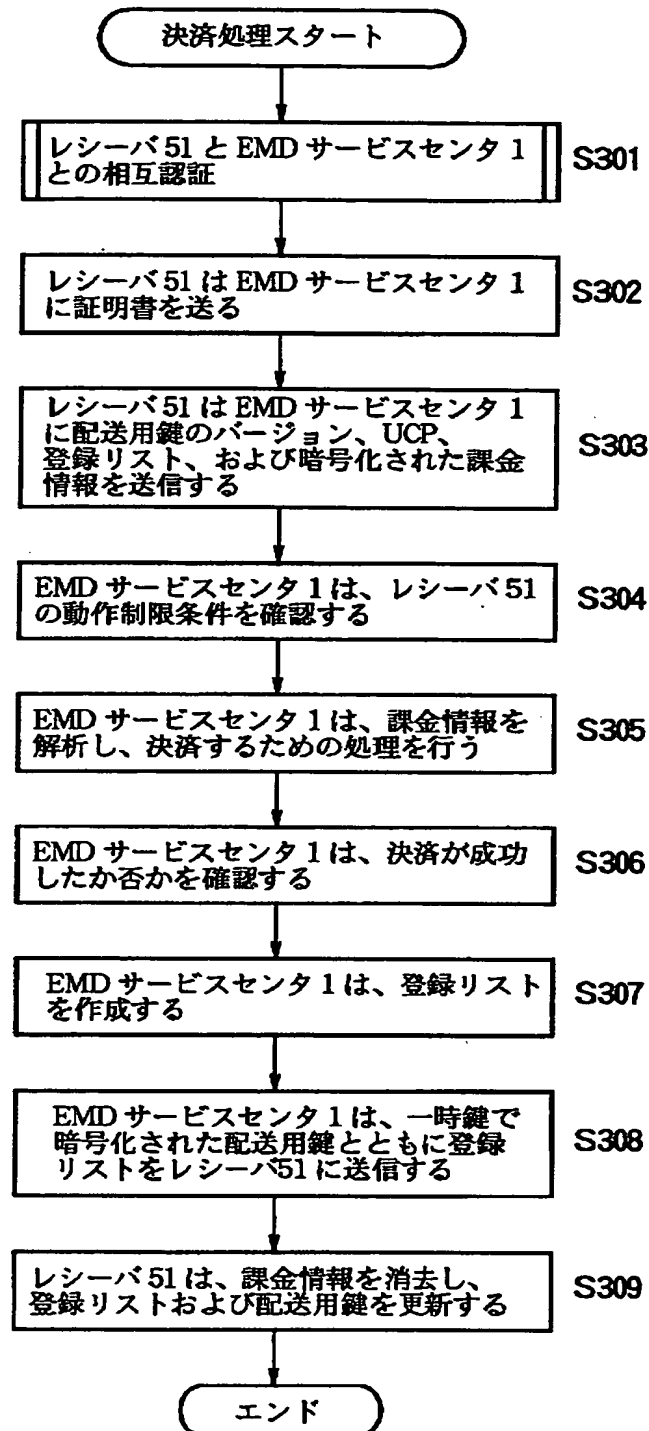
【図 4 6】



【図 47】



【図 48】



【書類名】 要約書

【要約】

【課題】 ユーザ情報に応じてサービスを提供できるようにする。

【解決手段】 PTA-1の「価格条件10」の「ユーザ条件10」には、男性のユーザであることが示されているので、PTA-1は、男性のユーザのみが選択可能となる。PTA-2の「価格条件20」の「ユーザ条件20」には、女性のユーザであることが示されているので、PTA-2は、女性のユーザのみが選択可能となる。PTA-1とPTA-2の価格内容を比較すると、PTA-2の価格内容に示される額は、対応するPTA-1の価格内容に示される額の半分にされている。すなわち、女性ユーザは、男性ユーザに比べ、半額の料金でコンテンツを利用することができる。

【選択図】 図20

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社



)